UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF PENNSYLVANIA

COMMONWEALTH OF PENNSYLVANIA, by Attorney General KATHLEEN G. KANE, Plaintiffs, v. THINK FINANCE, INC., TC LOAN SERVICE, LLC, ELEVATE CREDIT, INC., FINANCIAL U, LLC and KENNETH E. REES,WILLIAM WEINSTEIN, WEINSTEIN, PINSON AND RILEY, PS and CERASTES, LLC, NATIONAL CREDIT ADJUSTERS, LLC, SELLING SOURCE, LLC and PARTNERWEEKLY, LLC, d/b/a MONEYMUTUAL.COM, and other JOHN DOE person or entities, Defendants.	Civil Action No.

DECLARATION OF IRA N. RICHARDS IN
<u>SUPPORT OF DEFENDANTS' NOTICE OF REMOVAL</u>

I, Ira N. Richards, hereby declare:

1. I am an attorney licensed to practice law in the State of Pennsylvania and am admitted to practice before this Court. I am a partner with the law firm of Schnader Harrison Segal & Lewis LLP, counsel of record for defendants Think Finance, Inc., TC Loan Service, LLC, and Financial U, LLC. I submit this declaration in support of Think Finance, Inc., TC Loan Service, LLC, and Financial U, LLC's Notice of Removal, filed concurrently with this declaration. I make this declaration based on personal knowledge, except where otherwise indicated. If called as a witness, I would testify to the facts listed below.

2. Attached hereto as Exhibit A is a true and correct copy of a webpage, as of December 11, 2014, from the Federal Deposit Insurance Corporation's (FDIC) website entitled "FDIC: Confirmation & Report Selection," available at https://www2.fdic.gov/idasp/main.asp (change "Institution Status" to "All" and then search for "First Bank of Delaware").

3. Attached hereto as Exhibit B is a true and correct copy of the Order to Cease and Desist, Order for Restitution, and Order to Pay from *In the Matter of First Bank of Delaware, Wilmington, Delaware*, FDIC-07-256b and FDIC-07-257k.

4. Attached hereto as Exhibit C is a true and correct copy of Chapter XIV of a pdf document from the FDIC entitled "*Credit Card Activities Manual*," as of December 11, 2014, and available at https://www.fdic.gov/regulations/examinations/credit_card/pdf_version/ch14.pdf.

5. Attached hereto as Exhibit D is a true and correct copy of Chapter XIX of a pdf document from the FDIC entitled "*Credit Card Activities Manual*," as of December 11, 2014, and available at https://www.fdic.gov/regulations/examinations/credit_card/pdf_version/ch19.pdf.

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration was executed in Philadelphia, Pennsylvania, on this 16th day of December, 2014.

Ira N. Richards

EXHIBIT A

Key demographic information as of December 4, 2014

First Bank of Delaware
1000 Rocky Run Parkway
Wilmington,DE 19803

FDIC Certificate #:	34929	Date Established:	6/1/1999
Bank Charter Class:	Federal Reserve Non-member	Date of Deposit Insurance:	6/1/1999
Primary Federal Regulator:	Federal Deposit Insurance Corporation		
Primary Internet Web Address:	Web site not available.		

This is an inactive institution.

Inactive as of: November 16, 2012
Closing history: This institution was involved in a **Voluntary Liquidation and Closing**.
Acquiring institution: This action did not result in a new institution.

Information Gateway;

ID Report Selections: Assets and Liabilities

Report Date: September 30, 2012

More Information

- Current List of Offices not available
- Compare to Peer Group(s)
- FFIEC Call/TFR Report ***9/30/2012 Latest Available***
- FFIEC Uniform Bank Performance Report (UBPR)
- FDIC/OTS Summary of Deposits
- Bank Holding Company Ownership and Affiliates not available
- Regional Economic Conditions (FDIC RECON)
- Organization Hierarchy from the Federal Reserve System
- FDIC CRA ratings
- Consumer Assistance from Primary Federal Regulator

Press for description

EXHIBIT B

FEDERAL DEPOSIT INSURANCE CORPORATION

WASHINGTON, D.C.

In the Matter of FIRST BANK OF DELAWARE WILMINGTON, DELAWARE (INSURED STATE NONMEMBER BANK)	ORDER TO CEASE AND DESIST, ORDER FOR RESTITUTION, AND ORDER TO PAY FDIC-07-256b FDIC-07-257k

FIRST BANK OF DELAWARE, Wilmington, Delaware (Bank), having received a NOTICE OF CHARGES FOR AN ORDER TO CEASE AND DESIST AND FOR RESTITUTION; NOTICE OF ASSESSMENT OF CIVIL MONEY PENALTIES; FINDINGS OF FACT AND CONCLUSIONS OF LAW; ORDER TO PAY; AND NOTICE OF HEARING issued by the Federal Deposit Insurance Corporation (FDIC) on June 10, 2008 detailing the violations of law and/or regulations and unsafe or unsound banking practices alleged to have been committed by the Bank, and having been advised of its right to a hearing with respect to the foregoing under sections 8(b) and 8(i)(2) of the Federal Deposit Insurance Act (Act), 12 U.S.C. §§ 1818(b) and (i)(2), and the FDIC Rules of Practice and Procedure, 12 C.F.R. Part 308, and having waived those rights, entered into a STIPULATION AND CONSENT TO THE ISSUANCE OF AN ORDER TO CEASE AND DESIST,

ORDER FOR RESTITUTION, AND ORDER TO PAY (CONSENT AGREEMENT) with a representative of the Legal Division of the FDIC, dated October 3, 2008, whereby, solely for the purpose of this proceeding and without admitting or denying the alleged violations of law and/or regulations and unsafe or unsound banking practices, the Bank consented to the issuance of an ORDER TO CEASE AND DESIST, ORDER FOR RESTITUTION, AND ORDER TO PAY (ORDER) by the FDIC.

The FDIC considered the matter and determined that it has reason to believe that the Bank committed violations of law and/or regulations and engaged in unsafe or unsound banking practices, including, but not limited to, violations of section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (Section 5) and operating the Bank without effective oversight and supervision of the Bank's consumer lending programs.

The FDIC, therefore, accepts the CONSENT AGREEMENT and issues the following:

ORDER TO CEASE AND DESIST

IT IS HEREBY ORDERED, that the Bank, its institution-affiliated parties, as that term is defined in section 3(u) of the Act, 12 U.S.C. § 1813(u), and its successors and assigns, cease and desist from the following violations of law and/or

regulations and from engaging in the following unsafe or unsound banking practices:

(a) operating in violation of Section 5;

(b) operating the Bank's National Consumer Products Division (NCP Division) without effective oversight by the Bank's board of directors (Board) and supervision by senior management of the lending programs offered, marketed, administered, processed, serviced and/or collected by third-parties pursuant to arrangements or agreements with the Bank including, but not limited to, those third-party arrangements and agreements identified in Exhibit "A" of the CONSENT AGREEMENT (all collectively referred to in this ORDER as "third-party lending programs"); and any vendor, servicer or third party providing one or more of these functions or services material to the Bank's third-party lending programs (all collectively referred to in this ORDER as "third-party provider");

(c) operating the Bank's NCP Division with an inadequate system of internal controls, management information system, and internal audit system with regard to the size of the NCP Division and the nature, scope and risks of the third-party lending programs and third-party providers, in contravention of

the Standards for Safety and Soundness contained in Appendix A to Part 364, 12 C.F.R. Part 364;

(d) operating the Bank's NCP Division with an inadequate compliance management system to ensure compliance with Section 5 and other federal consumer protection laws and regulations; and

(e) operating the Bank with inadequate capital planning in relation to the risk considerations and/or factors prescribed by the *Interagency Expanded Guidance for Subprime Lending Programs* (FIL-9-2001, issued January 31, 2001) and the FDIC's *Credit Card Activities Manual*, Chapter XIV.

IT IS FURTHER ORDERED that the Bank, its institution-affiliated parties, and its successors and assigns, take affirmative action as follows:

I. TERMINATION OF THIRD-PARTY LENDING PROGRAMS AND RELATIONSHIPS WITH THIRD-PARTY PROVIDERS

Within sixty (60) days of the effective date of this ORDER, the Bank shall develop and submit to the Regional Director of the FDIC's New York Regional Office (Regional Director), for her non-objection in accordance with paragraph XIII.A of this ORDER, a comprehensive plan, with timelines, for the termination of all relationships with third-party providers and the termination of

all third-party lending programs or any agreements or arrangements with third-party providers that exhibit the characteristics of a "Rent-a-BIN" or "Rent-a-ICA" arrangement, as referred to in the FDIC's *Credit Card Activities Manual*, except for those third-party lending programs and third-party providers specifically identified in Exhibit "B" of the Consent Agreement. The plan shall provide for these terminations within one hundred and twenty (120) days of the effective date of this ORDER. Upon termination of each third-party lending program and/or the relationship with a third-party provider, the Bank shall provide written notification to the Regional Director apprising her of the date the third-party lending program or the relationship with the third-party provider was terminated.

II. NCP DIVISION PLANS

A. Consultant:

1. Within thirty (30) days of the effective date of this ORDER, the Bank shall retain an independent third-party consultant (Consultant) acceptable to the Regional Director with appropriate expertise and qualifications to assist the Bank with the preparation of a comprehensive strategic plan and an operating plan for the Bank's NCP Division (NCP Division Plans) as well as the assessment of management and staff needs within the NCP Division required by Article III and the Capital Plan

required by Article IV of this ORDER.

2. The Bank shall provide the Regional Director with a copy of the proposed engagement letter or contract with the Consultant for her review and non-objection. The contract or engagement letter, at a minimum, should include:

a. a description of the work to be performed under the contract or engagement letter;

b. the responsibilities of the Consultant;

c. identification of the professional standards covering the work to be performed;

d. identification of the specific procedures to be used when carrying out the work to be performed;

e. the qualifications of the employee(s) who are to perform the work;

f. the time frame for completion of the work; and

g. a provision for unrestricted access by the FDIC to the Consultant's staff, work papers and other materials prepared in the course of the Consultant's engagement.

B. Strategic Plan:

Within ninety (90) days of the effective date of this ORDER, the Bank shall, with the assistance of the Consultant, develop and submit to the Regional Director, for her non-objection in accordance with paragraph XIII.A of this ORDER, a comprehensive

strategic plan (Strategic Plan) covering an operating period of at least three (3) years. The Strategic Plan shall include, at a minimum:

1. a full and complete description of each and every consumer loan product (Consumer Product) and/or consumer lending activity the Bank will offer or in which the Bank will engage, either within the NCP Division or any other area or division of the Bank;

2. a full and complete list of each third party the Bank plans to utilize in connection with any Consumer Product or consumer lending activity, either within the NCP Division or any other area or division of the Bank;

3. a full and complete description of the function or service each third party will provide in connection with any Consumer Product or consumer lending activity, either within the NCP Division or any other area or division of the Bank; and

4. the planned volume and growth of each of these Consumer Products and/or consumer lending activities either within the NCP Division or any other area or division of the Bank.

C. <u>Operating Plan</u>:

Within ninety (90) days of the effective date of this ORDER, the Bank shall, with the assistance of the Consultant, develop and submit to the Regional Director for her non-objection in accordance with paragraph XIII.A of this ORDER, specific operating policies and procedures (Operating Plan) that appropriately take into account the nature, scope, and risk of each Consumer Product and each consumer lending activity whether offered or engaged in within the NCP Division or any other area or division of the Bank as well as the size of such divisions or areas of the Bank and address the following areas:

1. Internal Control System: The Bank's Internal Control System shall, at a minimum, include policies, procedures and processes that provide for:

a. an organizational structure for the day-to-day operation and oversight of the Bank's Consumer Products and consumer lending activities with (i) clear lines of authority and identification of reporting lines; (ii) clear assignment of responsibility along the lines of authority for assessing and monitoring the compliance of each Consumer Product and each consumer lending activity with all applicable federal consumer protection laws, including Section 5, and all implementing rules and regulations, regulatory guidance, and statements of policy

as well as all applicable policies and procedures of the Bank including, but not limited to, those specific areas of non-compliance noted in the FDIC's Report of Examination dated April 25, 2007 (ROE) and/or the FDIC's Compliance Report of Examination as of April 6, 2006 (Compliance Report); and (iii) clear assignment of responsibility for reporting to the Board the results of the assessment and monitoring activity performed under this subparagraph, including specification of information and data to be reported to the Board on a periodic, but not less than quarterly, basis;

b. initial and periodic, but not less than quarterly, written reports to the Board assessing the strategic, legal, reputational, transactional, compliance, regulatory, accounting and credit risk associated with each Consumer Product and each consumer lending activity; and

c. an adequate number of staff to ensure full and complete compliance with subparagraphs (a) and (b) above.

2. Management Information System: The Bank's management information system (MIS) shall, at a minimum, include policies, procedures and processes that provide for:

a. new or enhanced systems to allow the Bank to appropriately monitor each Consumer Product and each consumer

lending activity for compliance with all applicable federal consumer protection laws and implementing rules and regulations, regulatory guidance, and statements of policy as well as all applicable policies and procedures of the Bank;

b. new or enhanced systems to allow the Bank to access, collect and analyze such data, documentation or other information necessary for effective monitoring of each Consumer Product and each consumer lending activity;

c. new or enhanced systems to allow the Bank to access, collect, and analyze such data, documentation or other information necessary to calculate fee rebates due in the event a loan is prepaid;

d. new or enhanced systems to allow the Bank to access, collect, and analyze such data, documentation or other information necessary to determine whether installment loan products and similar products (ILPs) comply with the guidance set forth in the *FDIC's Supervisory Policy on Predatory Lending* (FIL-6-2007, issued January 22, 2007) including the ability to determine whether a lending transaction represents a fair exchange of value for the borrower and whether the pricing of the loan appropriately reflects the borrower's risk of repayment

and whether it is customary and reasonable under the circumstances; and

e. an adequate number of staff to ensure full and complete compliance with subparagraphs (a) through (d) above.

3. Internal Audit System: The Bank's Internal Audit System shall, at a minimum, include policies, procedures and processes that ensure:

a. adequate monitoring of the Internal Control System through a comprehensive internal audit function;

b. an audit staff comprised of a sufficient number of qualified persons;

c. the independence and objectivity of the internal auditor, the audit staff, and the audit committee;

d. adequate testing and review of MIS for the Bank's NCP Division and/or any other area or division of the Bank offering a Consumer Product or engaging in a consumer lending activity;

e. adequate testing and review of Consumer Products and consumer lending activities such that the scope and testing are adequate to (i) detect substantive deficiencies in the operation of the Bank's Consumer Products and consumer

lending activities; and (ii) determine the level of compliance of the Bank's NCP Division and/or any other area or division of the Bank offering Consumer Products and/or engaging in consumer lending activities with all applicable federal consumer protection laws and all implementing rules and regulations, regulatory guidance, and statements of policy as well as all applicable policies and procedures of the Bank;

f. adequate documentation of tests and findings of any corrective actions;

g. verification and review of management actions to address material weaknesses;

h. tracking of deficiencies and exceptions noted in audit reports with periodic, but not less than quarterly, status reports to the Board with each deficiency and material exception identified, the source of the deficiency or exception and date noted, responsibility for correction assigned, and the date corrective action was taken in the report;

i. review of the effectiveness of the NCP Division's Internal Audit Systems and/or the Internal Audit Systems of any other area or division of the Bank offering

Consumer Products or engaging in consumer lending activities by the Bank's Audit Committee or Board; and

j. an annual audit schedule for the NCP Division and/or any other area or division of the Bank offering Consumer Products or engaging in consumer lending activities approved by the Board with any planned changes to or deviations from the approved audit schedule, its scope, or content requiring the prior written approval of the Board or its Audit Committee appropriately reflected in the minutes of the meeting wherein the change or deviation was approved.

4. Compliance Management System (CMS): The Bank's CMS shall, at a minimum, include policies, procedures and processes that ensure that all Consumer Products and consumer lending activities comply with all applicable federal consumer protection laws, including Section 5, and all implementing rules and regulations, regulatory guidance, and statements of policy and provide for:

a. Bank review, approval (prior to first use and subsequent re-reviews as may be required by, among other things, regulatory guidance and changes in laws and/or regulations), and maintenance of copies of (i) all marketing and solicitation materials, including direct mail or Internet

solicitations, promotional materials, advertising, telemarketing scripts, (ii) other materials provided to consumers and accountholders generated in connection with the administration and servicing of the Consumer Products and consumer lending activities, including accountholder agreements, privacy policies, forms of accountholder statement, and (iii) changes or amendments with respect to the materials described in (i) and (ii);

b. timely and regular notification to the Bank by any third-party provider of all regulatory agencies' inquiries, customer complaint correspondence, and/or legal action received from any third party with respect to the Consumer Products and consumer lending activities (other than routine requests such as to cease and desist collection contact);

c. (i) Bank review and approval of all materials related to customer service and collection activities, including compliance with the guidance set forth in FDIC FIL-52-2006 (issued June 21, 2006), (ii) monitoring of customer service and/or collection calls on a regular basis, (iii) Bank review of service level reports, and (iv) procedures for promptly addressing and resolving customer complaints regarding the

Consumer Products and consumer lending activities, regardless of the source;

d. Bank review of periodic, but not less than quarterly, quality assurance reports, reports on collection results, collector evaluation results, and a summary of disciplinary action reports for each call center;

e. Bank review of all third-party lending program's and third-party providers' credit, fraud, and risk management materials, including policy manuals and practices, to determine compliance with all applicable consumer protection laws;

f. Bank review and approval of all materials in connection with any Consumer Products and consumer lending activities, including arrangements for Consumer Products between third-party providers and any other vendor or party providing material services to the third-party provider; and monitoring periodically, but not less than quarterly, reviews, including the review of quality assurance reports and on-site audits, of all such material service providers;

g. periodic, but not less than quarterly, review by the Bank of all account services materials, including

materials related to customer chargeback and dispute processing, mail forwarding, returned mail and copy requests;

h. Bank review and regular monitoring of all third-party providers' materials relating to suspense item research, general ledger reconcilement and settlement, including daily settlement reports and preparation of monthly settlement reports;

i. Bank review of all materials related to the financial performance of Consumer Products and consumer lending activities and monthly performance monitoring of assets relating to the Consumer Products and consumer lending activities as a whole and by vintage and campaign, including new accounts established, receivables growth or decline, charge-offs, credit risk scores (such as Fair Isaac & Co. (FICO) scores), sources of revenue (annual percentage rates (APRs) and fees), number of accounts receiving credit line increases and decreases, and APR increases or reductions;

j. Bank monitoring of the performance of marketing and solicitation programs for new accounts and enhancement products, including numbers of accounts offered, the products in each campaign and response rate, and production and review of trend analysis;

k. mandatory regular compliance reviews by the Bank, including all policies and procedures, and internal compliance audits and on-site visits to service facilities of all third-party providers;

l. Bank review of all business and strategic plans relating to agreements with third-party providers;

m. Bank maintenance of records of all approved consumer materials, complaints and responses, solicitation materials, administration materials, and service provider agreements, relating to the Bank's Consumer Products and consumer lending activities;

n. Bank maintenance of files documenting the service level standards for those services provided by third-party providers and their service providers, including due diligence reports, monitoring and audit results, and financial materials;

o. Bank scheduling and conducting regular meetings with its third-party providers, for which written minutes will be taken and maintained;

p. Bank monitoring of third-party membership programs, if any;

q. periodic, but not less than quarterly, Bank monitoring of the use and security of confidential and nonpublic personal information;

r. an effective training program that includes regular, specific, comprehensive training in applicable federal consumer protection laws, including Section 5, and all implementing rules and regulations, regulatory guidance and statements of policy, for appropriate Bank personnel; and

s. an appropriate number of compliance personnel with sufficient experience in, and knowledge of, Consumer Products and consumer lending activities and consumer compliance laws and regulations to administer the CMS.

5. Account Management: The Bank's policies, procedures and systems shall ensure compliance with the guidance set forth in the *Account Management and Loss Allowance Guidance for Credit Card Lending* (FIL-2-2003, issued January 8, 2003), and, at a minimum, shall include the following:

a. requirements that minimum payments will preclude negative amortization and will amortize the current balance over a reasonable period of time, consistent with the unsecured nature of the underlying debt and the consumer's documented creditworthiness;

b. establishment of policies and procedures that provide for reasonable control over and timely repayment of amounts that exceed established credit limits; and

c. to the extent that the Bank utilizes any third parties pursuant to contract or otherwise to provide any services for account management and/or account servicing, the Bank shall ensure that all such third parties comply with the requirements of subparagraphs (a) and (b) above.

6. Predatory Lending: The Bank's policies, procedures and systems shall ensure that its ILPs comply with the guidance set forth in the *FDIC's Supervisory Policy on Predatory Lending* (FIL-6-2007, issued January 22, 2007).

III. ASSESSMENT OF MANAGEMENT AND STAFF

A. NCP Division Consultant:

1. Within thirty (30) days of the effective date of this ORDER, the Consultant shall analyze and assess the Bank's management and staffing needs within the NCP Division. The analysis and assessment shall be summarized in a written report to the Board (NCP Division Report), with a copy simultaneously delivered to the Regional Director. At a minimum, the NCP Division Report shall:

a. identify the type and number of Senior

Executive Officers (as that term is defined in 12 C.F.R. § 303.101(b)) and other officer positions needed to appropriately manage and supervise the affairs of the NCP Division, detailing any vacancies and additional needs with appropriate consideration to the size of the NCP Division and the nature, scope and risks of (i) each Consumer Product and/or consumer lending activity; (ii) each third party utilized by the Bank in connection with any Consumer Product and/or consumer lending activity; and (iii) the Bank's remaining third-party providers and make such modifications as are sufficient to retain personnel with adequate experience to oversee the NCP Division;

b. identify the type and number of staff positions needed to implement the plans, policies, procedures and processes required by this ORDER, detailing any vacancies and additional needs;

c. identify the authorities, responsibilities, and accountabilities attributable to each position, as well as the appropriateness of the authorities, responsibilities, and accountabilities, giving due consideration to the relevant knowledge, skills, abilities, and experience of the incumbent, if any, and the existing or proposed compensation; and

d. present a clear and concise description of the

relevant knowledge, skills, abilities, and experience necessary for each position, including delegations of authority and performance objectives.

B. NCP Division Management Plan:

1. Within sixty (60) days of receipt of the NCP Division Report, the Bank will develop a written plan of action (NCP Management Plan) in response to each recommendation contained in the NCP Division Report and a time frame for completing each action. A copy of the NCP Management Plan and any subsequent modification thereto shall be subject to review, comment and non-objection by the Regional Director to ensure that the NCP Management Plan and any subsequent modification comply with the requirements of this ORDER.

2. The NCP Management Plan shall be adopted by the Board and implemented by the Bank in accordance with paragraph XIII.A of this ORDER.

C. Bank Policies and Procedures to Evaluate Performance: Within sixty (60) days of the effective date of this ORDER, the Board shall establish policies and procedures to periodically analyze and assess the performance of management and staff in the performance of their present duties and anticipated duties (Performance Plan). The Performance Plan shall be submitted to

the Regional Director for her review and comment and/or non-objection. At a minimum, the Performance Plan shall:

1. establish policies and procedures to evaluate the current and past performance of management and staff members of the Bank, indicating whether the individuals are competent and qualified to perform present and anticipated duties, adhere to applicable laws and all implementing rules and regulations, regulatory guidance, statements of policy, the Bank's established plans, policies, procedures and processes and operate the Bank in a safe and sound manner;

2. establish policies and procedures to recruit and retain qualified directors, Senior Executive Officers and personnel consistent with the Performance Plan's analysis and assessment of the Bank's management and staffing needs;

3. establish policies and procedures to provide for any additional training and development needs not specifically identified and required by this ORDER, as well as policies and procedures to provide such training and development to the appropriate personnel; and

4. establish policies and procedures that provide for periodic, but not less than annual, review and update of the

Performance Plan.

D. Board and Management Changes:

While this ORDER is in effect, the Bank shall notify the Regional Director in writing of any changes in any of its Senior Executive Officers or Board members. Such notification shall include a description of the background and experience of the proposed officer or Board member and must be provided thirty (30) days prior to the individual(s) assuming the new position(s).

IV. CAPITAL PLAN

Within ninety (90) days of the effective date of this ORDER, the Bank shall, with the assistance of the Consultant retained pursuant to Article II of this ORDER, develop and submit a written capital plan (Capital Plan) to the Regional Director for her non-objection in accordance with paragraph XIII.A of this ORDER. The Capital Plan shall require, at a minimum:

A. specific plans for the maintenance of capital in an amount adequate and appropriate for the Bank taking into consideration its Strategic Plan and consistent with the risk considerations and/or factors prescribed by the *Interagency Expanded Guidance for Subprime Lending Programs* (FIL-9-2001,

issued January 31, 2001) and the FDIC's *Credit Card Activities Manual*, Chapter XIV, Credit Card Issuing Rent-a-BINs;

B. projections for asset growth and capital levels based upon a detailed analysis of the Bank's current and projected assets, liabilities, earnings, fixed assets, and the risks associated with its off-balance sheet activities including, but not limited to, any "Rent-a-BIN", "Rent-a-ICA" or similar activities;

C. projections of the sources and timing of additional capital to meet the Bank's current and future needs;

D. the primary source(s) from which the Bank will obtain capital to meet the Bank's needs;

E. a contingency plan that identifies alternative sources should the primary source(s) under paragraph (D) above be unavailable; and

F. a dividend policy that permits the declaration of a dividend only when the Bank is in compliance with its approved Capital Plan.

V. REVIEW AND UPDATING OF PLANS

A. The Bank shall review and update the Operating and Capital Plans required by Articles II and IV of this ORDER on a quarterly basis, or more frequently if specifically required herein or requested by the Regional Director. Copies of these reviews and updates shall be submitted to the Regional Director for her review and non-objection in accordance with paragraph XIII.A immediately following their completion.

B. The Strategic Plan required by Article II of this ORDER shall be revised and submitted to the Regional Director for her review and non-objection in accordance with paragraph XIII.A of this ORDER forty-five (45) days after the end of each calendar year for which this ORDER is in effect.

VI. AFFIRMATIVE RELIEF

A. Corrective Measures:

Within ninety (90) days of the effective date of this ORDER, the Bank shall take all action necessary to eliminate and/or correct all violations and/or deficiencies noted in the ROE or the Compliance Report, including Section 5, and other federal consumer protection laws and regulations along with all contraventions of the federal banking agency policies and guidelines. In addition, the Bank shall take all necessary

steps to ensure future compliance with all applicable laws and regulations, including Section 5, and all other applicable federal consumer protection laws and all implementing rules and regulations, regulatory guidance, and statements of policy.

B. Compliance:

Within ninety (90) days of the effective date of this ORDER, the Bank shall take all action necessary to comply with the guidance set forth in *Unfair or Deceptive Acts or Practices by State-Chartered Banks* (FIL-26-2004, issued March 11, 2004). At a minimum, the Bank shall not make, directly or indirectly, any misrepresentation, expressly or by implication, about any material term of an offer or extension of credit including, but not limited to, the amount of available credit or the relationship between an offer or extension of credit and a debt repayment plan or the repayment of existing debt, in connection with the advertising, marketing, offering, soliciting, extending, billing or servicing of credit.

C. Disclosures:

The Bank shall, directly or indirectly, disclose as clearly and prominently as, and on the same page as, any representation about credit limits or available credit in any credit card

solicitation:

1. a description of:

a. all initial fees (Initial Fees), as defined below;

b. all other fees imposed for the issuance or availability of a credit card, or imposed based on account activity or inactivity, other than: (i) any fee imposed for an extension of credit in the form of cash; (ii) any fee imposed for a late payment; or (iii) any fee imposed in connection with an extension of credit in excess of the amount of credit authorized to be extended with respect to such account; or (iv) any fee imposed in connection with foreign country transactions or foreign currency exchange;

c. the amount and timing of all such fees; and

d. all other restrictions imposed for the issuance or availability of credit;

2. if the aggregate amount of the Initial Fees or other restrictions that affect initial available credit is material, the amount of credit available upon activation after application of the Initial Fees and other restrictions, *provided*

that if the solicitation offers a credit limit of "up to" a certain amount, the amount of available credit after application of Initial Fees and restrictions shall be expressed as an example of a typical offer of credit;

3. if the effect of the fees described in subparagraph 1.b or the restrictions described in subparagraph 1.d on available credit is material, a description of the effect of such fees or restrictions on available credit.

4. "Initial Fees" shall mean any annual, activation, account opening, membership, periodic, or other fee imposed for the issuance or availability of a credit card at the time the account is opened; *provided* that "Initial Fees" shall not include: (i) any fee imposed for an extension of credit in the form of cash; (ii) any fee imposed for a late payment; or (iii) any fee imposed in connection with an extension of credit in excess of the amount of credit authorized to be extended with respect to such account.

VII. ORDER FOR RESTITUTION AND OTHER RELIEF

IT IS FURTHERED ORDERED that:

A. The Bank shall establish and maintain an account in the amount of $700,000 to ensure the availability of restitution

with respect to categories of consumers, specified by the FDIC, who activated Tribute Little Rock, Imagine Little Rock, Purpose Advantage, and Embrace credit card accounts.

B. Any application of the account shall be made through a cash payment to or at the direction of the FDIC for the purpose of making restitution to consumers.

C. The FDIC may require the account to be applied under the following circumstances:

1. If CompuCredit Corporation, Atlanta, Georgia (CompuCredit) is required by a judgment, order or other agreement with the FDIC or the Federal Trade Commission (FTC), including an order or agreement issued or made pursuant to a settlement arrangement, to pay restitution (Required Restitution) to any consumers who activated Tribute Little Rock, Imagine Little Rock, Purpose Advantage, or Embrace credit card accounts, and CompuCredit defaults, in whole or in part, on its obligation to make the Required Restitution, the FDIC may require the account to be applied to the extent of such default.

2. If the FDIC and/or the FTC are unable to obtain a judgment, order or agreement requiring CompuCredit to pay restitution to any consumers who activated Tribute Little Rock, Imagine Little Rock, Purpose Advantage, and Embrace credit cards, because of a reason other than the merits of their claims

and despite making reasonable efforts to do so, the FDIC may require the account to be applied in full.

III. RESTITUTION PLAN FOR CONTINENTAL FINANCE CARD (CFC) PROGRAM

A. The Bank shall prepare a comprehensive restitution plan (CFC Restitution Plan) for consumers who, during the period from March 2006 to the effective date of this ORDER, applied in response to a communication that solicited applications for a CFC credit card and were approved (CFC Eligible Consumers). The CFC Restitution Plan shall require that the following fees charged to the accounts of CFC Eligible Consumers be credited to the consumer's account, and any resulting credit balance shall be refunded to the consumer in cash:

1. the $89 participation fee charged to those consumers who cancelled their accounts during the first two (2) billing cycles after the account was opened; and

2. for those consumers who accessed the Bank's website and made their first payment to their CFC credit card account online, the first $4 online payment fee.

B. The Bank shall hire a consultant, acceptable to the Regional Director, who may be a certified public accountant (CFC Consultant), who shall review and verify that the Bank accurately identified the CFC Eligible Consumers and correctly

credited the accounts of, and made cash refunds, as appropriate, to CFC Eligible Consumers.

C. The CFC Consultant shall prepare a detailed written report of the processes and procedures by which the Bank determined the restitution amounts described above in paragraphs VIII.A.1 and VIII.A.2. The report shall also include the following: (1) total number of CFC Eligible Consumers, (2) number of CFC Eligible Consumers who received credits and cash refunds, (3) total amount of credits made under the CFC Restitution Plan, and (4) total amount of cash refunds made under the CFC Restitution Plan.

D. Within one hundred and twenty (120) days of the effective date of this Order, the Bank shall implement the CFC Restitution Plan.

E. The report described above in paragraph VIII.C. shall be submitted to the Regional Director for her review and comment and non-objection in accordance with paragraph XIII.A of this ORDER within sixty (60) days after the Bank has completed implementation of the CFC Restitution Plan.

F. The Bank shall retain all records pertaining to the CFC Restitution Plan including, but not limited to: documentation of the processes and procedures used to determine

the CFC Eligible Consumers, the names, contact and account information of the CFC Eligible Consumers, any mailing records, and documentation that the appropriate credits and cash refunds were made.

IX. DIRECTORS' COMPLIANCE COMMITTEE

Within thirty (30) days of the effective date of this ORDER, the Board shall establish a Directors' Compliance Committee (Committee) reporting to the Board and responsible for overseeing the affirmative action required by this ORDER. The Committee shall be comprised of at least three (3) independent directors who shall not be employed in any capacity by the Bank other than as a director. The Committee shall monitor compliance with this ORDER and within ninety (90) days of the effective date of this ORDER, and every sixty (60) days thereafter during the life of this ORDER, shall submit to the Board for consideration at its next regularly scheduled meeting a written report detailing the Bank's compliance with this ORDER, including compliance with the enhanced independent audit program. The Committee's report shall be incorporated into the minutes of the corresponding Board meeting. Nothing herein shall diminish the responsibility of the entire Board to ensure compliance with the provisions of this ORDER.

X. PROGRESS REPORTS

The Bank shall furnish a written progress report to the Regional Director ninety (90) days after the effective date of this ORDER and every ninety (90) days thereafter, detailing the form and manner of all actions taken to secure compliance with this ORDER and the results of such actions. Such reports may be discontinued when the corrections required by this ORDER have been accomplished and the Regional Director has released the Bank in writing from making further reports. Nothing in this Article X shall relieve the Bank from compliance with any other reporting requirements or provisions of this ORDER. All progress reports and other written responses to this ORDER shall be reviewed by the Board and made a part of the minutes of the corresponding Board meeting.

XI. ORDER TO PAY

IT IS FURTHER ORDERED THAT, by reason of the alleged violations of law and/or regulations, and after taking into account the CONSENT AGREEMENT, the appropriateness of the penalty with respect to the financial resources and good faith of the Bank, the gravity of the conduct by the Bank, the history of previous conduct by Bank, and such other matters as justice may require, pursuant to section 8(i)(2) of the Act, 12 U.S.C. § 1818(i)(2),

a civil money penalty of THREE HUNDRED AND FOUR THOUSAND DOLLARS ($304,000) is assessed against the Bank. The Bank shall pay the civil money penalty to the Treasury of the United States. The Bank shall pay such civil money penalty itself, and is prohibited from seeking or accepting indemnification for such payment from any third party.

XII. NOTICE TO SHAREHOLDERS

Within sixty (60) days of the effective date of this ORDER, the Bank shall send to its shareholders or otherwise furnish a description of this ORDER. The description shall fully describe the ORDER in all material respects. The description and any accompanying communication, statement, or notice shall be sent to the FDIC, Division of Supervision and Consumer Protection, Accounting and Securities Disclosure Section, 550 17th Street, N.W., Washington, D.C. 20429 for review at least 20 days prior to dissemination to shareholders. Any changes requested to be made by the FDIC shall be made prior to dissemination of the description, communication, notice or statement.

XIII. MISCELLANEOUS

A. 1. Whenever a provision of this ORDER shall require the Bank to submit a proposed plan, policy, procedure or system; or an enhancement, revision or addition to a plan, policy, procedure, system; or other matter to the Regional Director for her review, comment and/or non-objection, the Bank shall make such submission to the Regional Director at 20 Exchange Place, New York, New York 10005.

2. The Regional Director shall provide comments to the Bank within thirty (30) days of receipt of the proposed plan, policy, procedure or system; or enhancement, revision or addition to the plan, policy, procedure or system; or other matter submitted for her review, comment and/or non-objection.

3. Within thirty (30) days of receipt of comments from the Regional Director, the Bank shall make such modifications as may be necessary to address the Regional Director's comments. If the Bank fails to make such modifications, or otherwise fails to address the Regional Director's comments within such thirty (30) day period, the Bank shall provide to the Regional Director a comprehensive written explanation, developed with its Consultant, of its rationale. Within thirty (30) days of receipt of the Bank's response, the Regional Director shall either (i) provide her non-objection to

the revisions proposed by the Bank; or (ii) provide comments as to her rationale for rejecting the proposed revisions, or such revisions which remain objectionable, and shall direct the Bank to implement the plan, policy, procedure, system, revision, or enhancement as finally approved.

4. The Bank's actions shall be appropriately recorded in the Board meeting minutes. Thereafter, the Bank and its directors, officers and employees shall fully implement and follow the plan, policy, procedure or other matter as adopted and shall ensure full and complete compliance with these plans, policies, procedures or other matters both internally and by any third party utilized by the Bank. It shall remain the responsibility of the Board to fully implement the plans, policies, procedures or other matters as adopted within the specified time frames.

5. If, after a reasonable period of time for implementation, the Bank has not complied with subparagraphs 1-4 above, the Regional Director may provide written notice of her objection(s) to the Bank and require the submission of a plan (Exit Plan) to discontinue its offering of the specified Consumer Product(s) or consumer lending activity. Within thirty (30) days of its receipt of the Regional Director's written

notice, the Bank shall develop and submit its Exit Plan to the Regional Director for her review and non-objection. The Exit Plan shall, at a minimum, provide for the discontinuation of the specified Consumer Product(s) or consumer lending activity within sixty (60) days of the Bank's receipt of the Regional Director's written notice.

6. The Bank shall not acquire any portfolios of consumer credit card accounts from any other insured depository institution or other entity until such time as the Bank has submitted, and the Regional Director has non-objected to, the plans, policies and procedures required under paragraphs I through IV of this Order.

B. The Bank shall use good faith reasonable efforts to cooperate with the FDIC in its pursuit of claims related to Tribute Little Rock, Imagine Little Rock, Purpose Advantage, and Embrace credit card products, including, upon reasonable prior notice and at reasonable times and places, in making its documents and records relating to the claims available to the FDIC (subject to any privilege or other protection available under applicable law) without subpoena and, upon reasonable prior notice and at reasonable times and places, in making its personnel (including officers, directors and employees)

available for interview and/or testimony by deposition or before any authorized tribunal without subpoena. The cooperation shall not require the Bank to waive any applicable privileges. The FDIC may use the documents and testimony in claims related to the Tribute Little Rock, Imagine Little Rock, Purpose Advantage, and Embrace credit card products, including any action brought by the FTC. Prior to their use in a proceeding, the documents and testimony will be kept confidential. Their use in a proceeding will be subject to confidentiality orders issued by the tribunal in which they will be used. The FDIC agrees to provide notice to the Bank if any third party other than the FTC attempts to obtain the documents or testimony.

C. Except for an action to enforce compliance with this ORDER and except for any claims against the CompuCredit Parties, as hereinafter defined, the FDIC shall not commence any action under section 8 of the Act, 12 U.S.C. § 1818, Section 5, or any other statute or regulation, against the Bank, or any of its directors, officers, employees, and agents, or any of the Bank's affiliates, their successors or assigns, or any of their respective directors, officers, employees, and agents (collectively, the Bank Parties), arising out of or related to the Tribute Little Rock, Imagine Little Rock, Purpose Advantage,

and Embrace credit card programs or relating in any manner to the ROE and/or the Compliance Report and related investigations, in each case to the effective date of this ORDER. The CompuCredit Parties shall mean CompuCredit, its officers, directors, employees, subsidiaries, successors and assigns, and any party having a contract with CompuCredit or providing services to or for the benefit of CompuCredit, with the exception of any of the Bank Parties.

D. 1. Except as limited by the CONSENT AGREEMENT and paragraph XIII.C above, this ORDER shall not bar, estop or otherwise prevent the FDIC or any other federal or state agency or department from taking any action against any of the Bank Parties or any of the Bank's current or former institution-affiliated parties, or any of their respective directors, officers, employees, and agents.

2. The FDIC expressly reserves all rights against the CompuCredit Parties. Nothing in this ORDER or in the CONSENT AGREEMENT shall require the FDIC or any other party to reduce, compromise, or otherwise limit any claims against the CompuCredit Parties.

3. Nothing in this ORDER or in the CONSENT AGREEMENT shall require the FDIC or any other party to reduce, compromise, or otherwise limit any claims because of any contractual or other commitments of the Bank to indemnify, defend, or hold harmless any of the CompuCredit Parties.

E. Nothing herein shall prevent the FDIC from conducting on-site reviews and/or examinations of the Bank, its affiliates, agents, service providers, and any other institution-affiliated parties of the Bank at any time to monitor compliance with this ORDER.

F. This ORDER shall be effective on the date of issuance.

G. The provisions of this ORDER shall be binding on the Bank, its affiliates, their successors and assigns, and any of their respective directors, officers, employees, and agents, and any of the Bank's current or former institution-affiliated parties, and any of their respective directors, officers, employees, and agents.

H. The provisions of this ORDER shall remain effective and enforceable except to the extent that, and until such time as, any provisions of this ORDER shall have been modified, suspended or terminated in writing by the FDIC.

Pursuant to delegated authority.

Dated at Washington, D.C., this 9TH day of October, 2008.

____

Christopher J. Spoth
Senior Deputy Director
Division of Supervision and
Consumer Protection

EXHIBIT C

XIV. CREDIT CARD ISSUING RENT-A-BINS

Banks are involved in many business lines that have varying competitive pressures and requirements for success. They are increasingly evaluating each line to determine whether it makes the most of the bank's strengths and is consistent with its strategic plans. As management considers these evaluations, it may decide to stop activities that are not profitable or that are too high-risk for its appetite in order to concentrate on activities that may be more profitable, that it and the bank may be better-suited for, or that are lower-risk. These types of evaluations have led to the development of many variants of the credit card lending model, one of which is a Rent-a-Bank Identification Number (BIN) arrangement. This chapter describes Rent-a-BIN (RAB) models and structures, highlights the risks of issuing RAB arrangements, and discusses risk-mitigating controls that management typically employs. Later sections of the chapter consider topics such as capital and accounting.

RENT-A-BIN MODELS AND STRUCTURES

With a RAB arrangement, a bank allows one or more other entities to conduct credit card activities with or through one of the bank's BINs[8], which is a number assigned by an Association to identify the bank for authorization, clearing, settlement, card issuing, or other processes. In return for allowing the use of its BIN, the bank receives a "rental" fee from that entity, hence the term Rent-a-BIN.

There are essentially two types of RAB arrangements: a credit card issuing RAB and an acquiring RAB. Each has a unique set of risks but both require the bank to have strong vendor-oversight programs. Acquiring RABs, which draw their names from the arrangement's feature of acquiring merchant contracts and cardholder transactions, are addressed in the Merchant Processing chapter, and issuing RABs, which draw their names from the arrangement's feature of issuing credit cards to consumers, are the focus of this chapter.

There are several common features among issuing RABs. In an issuing RAB arrangement a bank (as BIN owner) rents its right to offer credit cards that have the applicable Association's logo to a third party for a fee. The third party generally solicits prospective credit card customers and then provides approved applicants with a credit card. The bank is identified as the issuer of the card while the BIN-renter, or partner, and other sub-contracted participants may not necessarily be apparent to the cardholder. The bank retains its contract with the Association(s) because the Associations only allow insured depository institutions to issue credit cards under their brands. While the bank sheds itself of a majority of the day-to-day operational duties associated with operating the program in most cases, it always retains ultimate responsibility for the program based on its contract with the applicable Association and on it being the issuer of record.

Issuing RABs also have several aspects that vary from arrangement to arrangement. For example, the receivables are usually held by the BIN-renter (partner) or another party. In a few cases the bank might hold a small portion of the receivables or even a majority or all of the receivables. Securitization of the program's receivables (by whichever party has funded those receivables) may or may not be present. In most cases, the partner is unaffiliated with the bank. However, the partner may be an affiliate of the bank or a related interest of an insider of the bank, requiring an additional layer of review. Furthermore, some banks have arrangements with more than one partner for different credit card programs/BINs. Portfolio services such as collections,

---

[8] As mentioned in an earlier chapter, an ICA is a number assigned by MasterCard and is similar to a BIN that is issued by Visa. ICAs and BINs are collectively referred to as BINs in this manual. This chapter references arrangements involving the Associations; but, similar arrangements may be encountered with other networks going forward, particularly now that Discover and American Express are expanding their bankcard markets.

customer service, and processing, can be performed by the partner or by other third-parties (which, again, may or may not be affiliated with the bank). The bank could even perform select services or processes. In most cases the bank is an issuer only, but it is plausible that it could be both issuing and acquiring, which could complicate matters (refer to the Merchant Processing chapter for information on the acquiring business).

A bank might enter into an issuing RAB to reduce or to limit the level of receivables held on its balance sheet (thus reducing or limiting on-book credit risk) and/or to reduce or limit the operating burden on internal resources while still generating income from credit card activities. While issuing RAB arrangements can be effective means of meeting these goals, they pose a number of risks to the bank, and those risks can be substantial. Problems commonly arise when management is overly focused on apparent returns or cost savings or when it lacks sufficient knowledge about the risks involved with the card products offered, RAB activities, and/or third-party oversight.

A primary concern with RAB arrangements is that the bank may not have sufficient controls over the partner's (or the partner's agent's) actions, particularly solicitation, underwriting, and administration of the credit card relationships. The quality of services provided by the hundreds of third-parties in credit card and related industries, as well as their wherewithal to support the activities, varies widely. If the partner or its agents fail to abide by applicable laws, guidance, and regulations, or if the partner experiences financial difficulties, the bank could be exposed to operation and reputation risks that may result in fines or other monetary losses, funding or liquidity risks if the partner or other receivable-holders are not able to provide funding for new charges that they have committed to fund, and credit risk if the bank must fund the cardholder charges and retain the receivables on its balance sheet. Credit risk, whether from receivables voluntarily retained or that the bank is forced to retain, could be substantial if the bank has not had proper control over the partner's underwriting criteria and the partner solicited and accepted customers with riskier profiles than what the bank would normally accept.

For purposes of this chapter, a simple structure will be used: the bank will be an issuer (and not an acquirer) and will generally be assumed to be contracting with one partner, and that partner will hold all card receivables as well as perform all servicing and processing for the portfolio. However, examiners should keep in mind that a bank may have more than one partner, that the partner might have relationships with more than one bank, that the bank may or may not retain the receivables, and that servicing may be performed by the partner, the bank, or another third-party. Examiners will need to review governing documents for issuing RAB arrangements (normally for those that are material or new) to ascertain the parties involved, the extent of each party's responsibilities, and how and to what degree failure of each party to meet its obligations may impact the bank, whether directly or indirectly. Examiners should also look for evidence identifying whether management has properly addressed the risks from each RAB arrangement.

RESPONSIBILITIES OF BANK MANAGEMENT

Management sometimes assumes that it does not have to carefully monitor the card portfolio, namely when the bank does not hold the receivables. However, in an issuing RAB arrangement, the bank is responsible for the program and its customer relationships regardless of where the receivables reside. Further, the performance of the accounts can substantially impact the risks to the bank. Another misconception is that if a contract is in place between the bank and the partner, the bank is sufficiently protected. Contracts, a necessary component of a successful RAB operation, may not always be iron-clad. For example, the partner's indemnification contribution is only as strong as its financial wherewithal. Further, in some situations the bank might step in and relieve the partner from some of its responsibilities under the contract, thus tainting the contract. As another example, even though the contract might call for the partner to reimburse fines, it is up to the bank to seek that reimbursement and it might elect not do so, perhaps to keep the third party viable or to avoid disruptions to the program. That is not to say that a partner could not also provide services or financial support beyond contract specifications.

Even though the bank might not be directly involved in solicitation, underwriting, and administration processes under the issuing RAB arrangement, it is still the legal owner of the card accounts and relationships. As the BIN-licensee, the bank is responsible to the Association(s) for transactions processed and/or cards issued with its BINs, and, thus, program oversight. Even though contracts between the bank and the partner might direct the partner to assume these and other responsibilities, regulatory agencies and, most likely, the Associations regard the bank as ultimately responsible for the program. Typically the Associations have nominal direct contact with the bank's third parties. Rather, the bank is responsible for managing the third-party relationships, ensuring the third party meets established standards, and looking to the partner for reimbursement or other support provided for in the contract between the bank and the partner. The Association(s) may look to the third party if the bank is unable to meet its obligations.

Rigorous and thorough oversight of issuing RAB arrangements is warranted for management to ensure the risks are appropriately controlled. Issuing RAB relationships should generally be subject to risk management, consumer protection, and other policies and practices consistent with those that would be used if the bank was issuing the cards directly. The assessment of controls, safeguards, and practices for RAB activities is factored into the Management component rating (and other component ratings as applicable).

RISKS

Issuing RABs can be profitable ventures but do entail risks which, if not properly controlled, can quickly erode profitability and/or cause many other problems, some of which could be critical, for the bank. Because the bank does not usually hold the preponderance of the receivables and because third parties are typically conducting most of the portfolio services, the risks may not appear as straightforward as they are with a conventional credit card lending model. The frequency and level of each risk to a RAB bank is influenced by a number of factors, including, but not limited to, the type of card program, the bank's experience with the program or similar programs, and the third party's experience with similar activities. Poor planning, oversight, and control by management and inferior performance or service by the partner are usually the culprits that increase the risks.

Due to the risks involved, RAB arrangements warrant carefully-orchestrated, management-appointed safeguards and controls. Examiners should determine whether management, even if only considering establishing an arrangement, is fully aware of the risks involved. They should look for evidence that management has identified and documented the business's risks as well as the expertise and controls that will be required to manage those risks. A formal risk assessment may be warranted, particularly when proposed RAB activities will be of a substantial volume or would involve higher-risk characteristics, such as subprime lending or new products. Risks with an issuing-RAB arrangement include, but may not be limited to, legal, compliance, and reputation risks; counterparty risk; funding risk; credit risk; and operational risk.

Legal, Compliance, and Reputation Risks

Legal, compliance (consumer or otherwise), and reputation risks are prominent in issuing-RAB arrangements. These risks can be particularly substantial when subprime lending or other high-risk activities are involved. While these three risks often go hand-in-hand, they are not synonymous. These types of risks arise because the bank is responsible for the program, including actions taken (or inaction) by the third-parties involved. The bank cannot effectively detach itself from the credit card activity since the bank's name remains as the card issuer and the bank remains contracted with the Associations. Thus, errors and violations of law or of cardholder agreements, by the bank or its contracted parties, could expose the bank to substantial monetary loss through lawsuits, fines, or other financial burdens. Consumer compliance risks, which can easily translate into safety and soundness risks, can be exacerbated

when the partner's (or its agents') employees interact directly with the bank's customers. For example, if marketing of the card program by the bank, the partner, or a third party is determined to be unfair or deceptive, the bank may be held responsible for any monetary penalties, reimbursements, and any other actions (such as shutting down the program) necessary to promptly address the concerns. As a result, risks to the bank's earnings and capital could ensue. The bank's reputation can also suffer by association with improper or abusive business practices conducted by the partner or its agents. Third parties' decisions may affect a bank's ability to establish new relationships or continue existing relationships, which could impact the bank's strategic objectives.

In general, the bank and its credit card programs must remain compliant with laws, regulations, and guidance including, but not limited to, the *Account Management and Loss Allowance Guidance for Credit Card Lending* (AMG), consumer protection laws, and anti-money laundering laws. The AMG is generally applicable to all insured institutions that offer credit card programs, regardless of whether or not the receivables are held at the bank. Further, banks' obligations to comply with the Associations' standards are not limited by the receivables' place of residence.

The Associations are highly cognizant of their own reputations. If the card program demonstrates increasing or high risk, inadequate controls, or high volumes in relation to the bank's size and resources, the Associations may require the bank to put up additional capital or collateral for the card program, regardless of where the receivables reside and regardless of whether or not a RAB arrangement is involved. Abuses of a bank's Association membership (including of the by-laws and operating regulations thereof) by a partner or its agents could also cause the bank to lose its authority to issue cards under the Associations' brands. Such a loss could impact the bank's reputation, earnings, and liquidity; could ultimately translate into capital problems for the bank; and/or could require substantial revisions to the bank's strategic objectives.

Regulators may also require augmented capital levels. The necessary level of capital is based on a number of factors, as discussed later in this chapter.

Counterparty Risk

Counterparty risk, or default risk, is the risk that the partner will fail to perform on its contractual obligations. It often ties closely to performance of the card portfolio because the partner's earnings and, thus, capital maintenance, formation, and support, is frequently a product of income generated by and costs associated with the program. The partner usually retains most of the program's income and carries most of the costs when it holds most or all of the receivables.

The partner could fail to meet its obligations under the contract(s) governing the RAB arrangement. For example, the partner might fail to fund the receivables, pay the rental fee, comply with established financial covenants and/or portfolio parameters, or maintain sufficient collateral support. As a result, the bank could have to fund the receivables, potentially increasing its liquidity, credit, and other risks. The bank might not be able to offset its oversight, management, or other costs for the program, which could stress the bank's earnings performance and, consequently, capital.

Funding Risk

Funding risk stems from the bank's responsibility to ensure that settlement[9] requirements are met. Funding risk, however, could be considered, in some respects, to be a by-product of

[9] Settlement is the term used to refer to the exchange of the actual funds for the cardholder transactions and associated fees. The issuers normally remit funds, through the Associations, to the acquirer, and the acquirer pays the individual merchants. Settlement is discussed in the Merchant Processing chapter.

counterparty risk. Usually the bank settles directly with the processor, whether or not the bank retains the receivables. Even if the partner or other third party is required by the RAB contract to fund settlement and/or may be able to settle directly with the processor, the bank is ultimately responsible to the Associations for ensuring settlement is met as it is the BIN-licensee and the issuer. Consequently, when funds available from the partner, which are usually influenced heavily by cardholder payments, cannot fully meet settlement requirements, the bank is looked upon to make up the difference.

Further, when the partner possesses the receivables, it could subsequently be selling those receivables via securitization. The securitization vehicle must be maintained whether or not the partner is able to fund or acquire the receivables and sell receivables to the securitization vehicle. Further, poor performance of the securitized portfolio could trigger cash capture or early amortization. In these cases, the trust will use incoming cardholder payments as applicable to fund **spread accounts**, pay off the investor certificates, and so forth. Since those funds will not be available to the partner to fund settlement, the bank could have to furnish funds.

Credit Risk

Credit risk remains at the bank for any receivables it retains. Credit risk also arises, albeit off-balance sheet or contingent, if receivables are held by the partner or another entity. Credit risk could shift to the bank if the receivables-holder cannot fulfill its financial obligations, such as settlement, and could be substantial if the bank has not properly controlled the partner's underwriting criteria and the partner has solicited accounts with risky profiles.

Operational Risk

Operational risk is generally defined as the risk of monetary loss resulting from inadequate or failed internal processes, people, and systems or from external events. Examples include fraud, business disruption, and poor execution of process management and can all have adverse impacts on the bank and its RAB programs. Comprehensive due diligence and contingency planning, including stand-in arrangements, can help limit the level of and impacts from operational risk.

RISK-MITIGATING CONTROLS

Practices and safeguards that management commonly implements to mitigate risks include, but are not limited to, instituting policy controls, performing due diligence procedures, establishing a comprehensive contract between the bank and the partner, and developing detailed contingency plans. Without proper safeguards in place, exposure could be substantial.

Policies

As part of being contractually responsible for and controlling the program, management normally establishes a thorough review and approval process for policies proposed or used by the partner. An effective RAB contract sets forth the bank's expectations regarding the partner's operating policies applicable to the program and provides bank management with the stated authority to periodically review the policies (both prior to and after implementation) to ensure the policies are consistent with the bank's standards and risk tolerances. Examiners should determine whether policy reviews are well-documented and whether a formal agreement process for program policies is used.

Examiners' attention should be directed to situations in which the bank's internal policies fail to specify a system for approving partners and an ongoing program to monitor the partner's financial condition and operating performance as well as portfolio performance. In general, a comprehensive policy designates the criteria for selecting partners, stipulates information that is

required in the RAB contract, and addresses other items, such as limits per RAB relationship and concentration limits.

Examiners' attention should also be directed to cases in which policies (whether the bank's or the partner's) are not consistent with the scale of the activity and the risks it presents. Typically the bank does not diverge from its normal lending practices when participating in RAB relationships. But, if the bank significantly diverges from its normal lending practices, examiners should assess how management has ensured that any eased standards still result in an acceptable level of credit risk and that any elevated risks are appropriately addressed. Failure to adequately control policies used by the partner could result in compliance and legal risks to the bank. Further, it could cause the partner to take on more risk, including credit risk, than it can control, and that risk could fall back on the bank if the partner is unable to meet certain financial obligations.

Due Diligence

Risk exposures generally increase when the bank is contracting with a disreputable or inexperienced partner. As is the case for any third-party arrangement, selecting a competent, qualified, and reputable partner is essential to effectively managing the arrangement's risks. Examiners should look for evidence that the due diligence process is structured to identify qualitative and quantitative aspects, both financial and operational, of the partner and to assess the arrangement's consistency with the bank's strategic goals. To be effective, due diligence should occur before conducting business or contracting with the entity, and at appropriate intervals thereafter, such as when the contract is due for extension or renewal.

Facts should corroborate that, before entering into or re-negotiating a RAB agreement, management ensured that the prospective partner had adequate financial capacity, expertise, infrastructure, technology, and staffing to operate the program soundly. In general, a thorough due diligence process includes documentation of these items:

- Analysis of credible financial information on the entity as well as its principals to verify the entity's viability and capacity to absorb losses.
- Research of background information and reputations of the entity and its ownership. This process may include reviewing business reputation, complaints, and litigation (such as by checking references or contacting attorney generals' offices and Better Business Bureaus). The length of time the entity has been in business is also applicable.
- Performance of a first-hand, on-site evaluation of the entity's business operations, including its premises and relevant records, to ensure it has the proper facilities, equipment, personnel, and so forth.
- Review of the entity's management experience in implementing and supporting the proposed activity as well as other relevant qualifications.
- Evaluation of the entity's business resumption, continuity, recovery, and contingency plans.
- Assessment of the entity's reliance on and success at dealing with sub-contractors, and resolution of which sub-contractors management will conduct due diligence of.
- Determination of whether appropriate insurance coverage is in place.
- Assessment of whether the entity's culture, values, business style, and strategies fit with the bank's culture, values, business style, and strategies.

In-House Expertise

Because of the risks associated with issuing RABs and to ensure the RAB operates successfully, it is imperative that the bank devote knowledgeable staff to oversee the arrangement. Examiners should assess the board of directors' practices for identifying the bank positions needed and clearly assigning responsibility for overseeing the partner and its operations. They should

determine whether the bank has provided adequate personnel and resources to fulfill its obligations in regards to the program and to monitor the partner's activities and portfolio performance. Examiners should look for proof that the bank's designated staff is knowledgeable and experienced with the processor, software programs, and other devices used by the partner and has legal and compliance expertise as well as accounting and technology expertise relevant to credit card lending. If the bank services the portfolio, proof should confirm whether it has adequate resources, expertise, infrastructures, and technology to appropriately provide the contracted services.

Contracts

Contractual responsibilities are fundamental to protecting the bank's interests and to determining the level and type of risks the arrangement brings to the bank. Effective contracts detail each party's responsibilities, specify what activities the partner is permitted to conduct, and are updated as needed. They also address the risk factors identified during the bank's risk assessment and due diligence processes. Normally, bank counsel reviews the proposed contract. Examiners should look for evidence that the contracts are structured to provide for the sound operation of the program as well as compliance with the Associations' standards. The level of protection offered by the contract could be questionable if the bank does not require the partner to consistently abide by its provisions, which normally cover, among other items:

- Financial reporting.
- Covenants and parameters.
- Access to information.
- Materials and program control.
- Settlement reserves (collateral protection).
- Pricing.
- Ability to terminate contract.
- Audit.

Financial reporting:

As noted, the bank is liable for meeting the settlement requirement daily but may look to the partner to supply settlement monies. Further, many RAB contracts contain indemnification provisions, but indemnification by the partner is only as strong as the financial wherewithal of the partner. A partner's financial situation could quickly become stressed, even to the point where it may file bankruptcy or become insolvent, possibly resulting in the bank having to retain the receivables if it had not been doing so already. The bank could possibly also end up having to cover costs, such as if fines or penalties have been imposed, if the partner cannot properly reimburse the bank according to governing contract provisions. As such, contract verbiage normally requires the partner to provide reliable financial information, including balance sheet, earnings, cash flow, and contingent liability information. Examiners' attention should be directed to situations in which the frequency of financial statement submission and review is not commensurate with the risk posed by the program and/or the partner. Partners are typically required to submit financial statements at least quarterly and audited financial statements annually. For higher-risk programs or higher-risk partners, more frequent submission and review may be required. Examiners should see proof that the board of directors has assigned responsibility both for evaluating the financial information and for reporting the findings to the board (or a designated committee) to competent employees. Contracts that require proper financial reporting practices can help the bank mitigate the risk of operating under a contract and program that is not fully supported by the financial wherewithal of the partner.

Covenants and parameters:

Contracts normally contain financial covenants for the partner (such as capital requirements, liquidity expectations, and appropriate settlement reserve balances) as well as card portfolio parameters (such as growth restrictions and performance expectations). The partner is usually required to periodically report and certify compliance with the covenants and parameters, and the contract normally prescribes remedies in the event the covenants and/or parameters are violated. Examiners' attention should focus on situations in which management does not have access to and/or does not review reliable data to monitor and test compliance with the established covenants and parameters. Proper examiner attention should also be given to situations in which review of the partner's budgets and other projections is not occurring. Such reviews help to detect trends that might signal emerging problems with meeting the covenants and parameters in the future. Further, situations in which the partner has violated the covenants or parameters warrant review during the examination.

If the portfolio becomes stressed, the partner (if it holds the receivables) could experience reduced cash flows which may, in turn, affect its ability to meet settlement requirements and, thus, potentially require the bank to provide funding. Portfolio deterioration could lead to a weakening of the partner's overall financial condition since a substantial portion of its earnings performance usually depends on the portfolio. Further, portfolio deterioration could signal ineffective servicing and management of the portfolio by the partner or other contracted servicers and could eventually entice the partner to use overly aggressive collection or other questionable servicing techniques, which could exacerbate compliance and legal risks. If the partner does not maintain appropriate capital or other financial measures, it may not be able to make good on its indemnification obligations and may not be able to fund the receivables. Thus, if contracts do not establish financial covenants for the partner as well as portfolio performance parameters for the portfolio, the bank is left with the risk that the partner may not be able to properly perform its contracted obligations, such as purchasing receivables, paying the rental fee, and so forth.

Access to information:

To ensure that management can assess the partner's policies and practices for compliance with laws, rules, regulations, safe and sound business practices, and the Associations' rules, the contract ordinarily provides management with ready access to such policies and procedures. Examiners should confirm whether procedures have been established to notify the bank when service disruptions, security breaches, or other events pose risk to the bank or when the partner receives any consumer complaints or litigation notices related to the bank's program. If a contract does not provide for appropriate access to information, the bank may be at the risk of unknowingly being named in lawsuits or unknowingly having its customers' or other information breached. A lack of appropriate access could also inhibit the bank from promptly identifying any changes that the partner may have inappropriately made to its policies or operating procedures.

Materials and program control:

The agreements generally grant the bank pre-approval rights over all program materials (such as marketing materials and cardholder agreements). Pre-approval rights over plans to issue new products or to materially alter existing products are also typical control features. Further, review and approval of card fee structures prior to implementation is a critical function of bank management. The granting and exercise of all of these rights is necessary to ensure that the partner is not taking on inappropriate levels of risk that could ultimately impact the bank. Contracts that are structured to commit the bank to open or maintain any particular level or number of cards, accounts, or receivables could cause the bank or the partner to take on a greater level of risk than can be appropriately controlled.

Settlement exposure reserves (collateral protection):

The contract ordinarily requires the partner to provide some kind of security or protection against any settlement exposure that the bank might face if the partner is unable to settle through agreed-upon normal means. Normal means could include the partner wiring funds to the bank daily, an authorized debit of the partner's general operating account at the bank, or some other similar method. Security for the exposure if the partner is not able to settle via normal means frequently takes the form of a combination of two or more of the following options: a deposit account, a contingency reserve, a credit facility, or other mechanism. Some banks have required the partner to hold ten days of coverage in aggregate. In any case, the funds available to the bank should tie to a realistic, well-documented contingency plan. The portfolio's available credit (open-to-buy) position and trends in that position can point to potential future trends or worst-case exposures regarding settlement activity, and, thus, are important considerations for determining the adequacy of protection provided. Settlement exposure reserves frequently consist of two items:

- *A Deposit Account* - Many contracts call for the partner to provide for and maintain an adequate deposit to cover potential shortfalls that may occur in daily settlement. This deposit is normally separate from any operating accounts that the partner might have at the bank. Concern arises when the method for determining the necessary deposit amount has not been specified or controlled by the bank. The deposit is usually held at the bank, but, whatever the case, examiners should look for evidence that the bank has proper controls over the deposit, which may include a perfected first lien. The partner typically has outside financing, so without proper controls, the bank's lien could fall behind liens of the financier. The deposit is usually required to cover several days of settlement volume (for purchases, cash advances, and so forth). Some contracts call for coverage of three days of volume (when a contingency reserve or other reserve/protection source is also used). Each contract needs to be reviewed on a case-by-case basis in the context of the activities being conducted and of any additional support (or lack thereof) provided by other means. Effective calculations to determine the deposit consider items such as seasonal fluctuations, portfolio growth, and customer payment rates and are well-documented. Contract features also usually call for the partner to replenish the balance in the account within a very short period once the account is drawn on. Compliance with the deposit requirement is often included in covenant-monitoring reports. Failure by management to ensure the deposit is accurately calculated and sufficiently funded could lead to an inability to meet settlement needs without the bank providing funds.

- *A Contingency Reserve* - Contracts also frequently require the partner to fund and maintain (at the bank or at a third-party) an adequate contingency reserve (or similar instrument) for use if the partner is unable to fully replenish the deposit account. Like the deposit, a contingency reserve usually covers several days of settlement, although its coverage is ordinarily longer, such as around seven days. Contingency reserves also warrant review on a case-by-case basis. In lieu of a contingency reserve, some partners establish a credit facility to the benefit of the bank. An effective contingency reserve calculation (or credit facility or other instrument) considers items such as seasonal fluctuations, portfolio growth, and customer payment rates and is well-documented. If the contingency facility is at a third party, examiners should evaluate management's practices for periodically verifying the availability and liquidity of the funds. Contracts may call for the partner to replenish these secondary funding sources within a very short period in the event they are drawn on, although if the contingency reserves are being drawn on, the third party is likely under financial stress. Failure to ensure the availability of such funds or the adequacy of the required funding amount could lead to an inability to settle in the event the bank does not step forward with its own funds. Again, proper controls over the contingency instrument are critical.

Pricing:

Comprehensive contracts clearly depict the compensation structure, allow for periodic review and re-pricing of services, and identify which party is responsible for each expense incurred. If the partner or another entity holds the receivables, a bank essentially pays for perceived insulation from credit losses by foregoing higher compensation that would typically be associated with carrying the card portfolio on its books. Rather, in these cases, the partner typically retains most of the income generated by the portfolio and carries most of the expenses. Examiners should evaluate whether the bank's compensation is commensurate with the risks retained as well as with the costs incurred for monitoring and managing the arrangement.

Ineffective pricing structures could quickly erode the bank's profits. Therefore, examiners should determine whether, prior to entering into or re-negotiating a RAB contract, management performs detailed cost analyses of its expenses and tries to obtain information on comparable transactions. Because the responsibilities and card portfolios under each bank's arrangements are different, pricing structures are difficult to compare and vary from contract to contract. Some contracts specify tiered fee structures where the fee per account (the definition of account also varies from contract to contract) is reduced as the volume of accounts increases. For example, a contract might call for a dollar per account for the first 100,000 accounts, 75 cents per account for the next 200,000 accounts, and so forth[10]. Others use a flat monthly rate. Some contracts call for an upfront fee (or set-up fee) and/or establish a minimum fee per month. Whatever the case, examiners should expect pricing to adequately compensate the bank for its risks and costs.

Examiners should also expect that, throughout the life of the arrangement, management produces an income and cost statement for issuing RAB activities and properly budgets for its RAB activities. Effective statements display RAB fees or other related income received and all direct and indirect costs incurred. The bank might have to make a sizeable investment in the program to implement systems and personnel to appropriately run and monitor the program. And, it might not be a profitable venture for the bank if the RAB partner is unable to generate a sufficient volume of accounts or properly manage the program.

Examiners' attention should also be directed to situations in which management is not monitoring portfolio profitability, regardless of whether the bank holds the receivables. Portfolios that evidence deteriorating or negative earnings performance could signal improper management by the partner, existing or future stressed cash flows to the partner, or other impacts on the partner, all of which could potentially, albeit indirectly, result in safety and soundness risks to the bank.

Ability to terminate contract:

Comprehensive contracts address circumstances under which the bank can exit the agreement and set forth reasonable timeframes for such actions. For example, the bank normally has the ability to terminate the contract if the partner materially breaches the contract (usually after considering a reasonable cure opportunity). Timeframes for notification of intent to terminate should be commensurate with the risks and the reasons for termination. Contract language that requires the bank to incur substantial fees for terminating the contract for appropriate cause should be carefully analyzed. Contracts that do not provide the appropriate ability to terminate the contract leave the bank at the risk having to operate a program that could be unprofitable or that has substantial liquidity risks or other implications.

Audit:

The potential for serious or frequent violations and noncompliance exists when a bank's oversight program does not include appropriate audit features. As such, management normally retains the right to audit the partner (and its sub-contractors). Contract verbiage also normally requires the

---

[10] The fees cited here are for example purposes only and should not be construed to be typical or endorsed pricing.

partner to provide its applicable internal and external audit reports, including the findings of financial and procedural audits and the partner's responses thereto, to bank management for review. If a contract does not provide for appropriate audit access, it leaves the bank at risk of failing to timely identify concerns or problems with the program and its operations. As a result, the bank could become subject to elevated legal, compliance, or other risks.

Examiners should look for proof that the bank's internal audit program incorporates a comprehensive review of bank management's supervision and oversight of the RAB relationships and activities as well as a review of each entity's adherence to contract provisions. The bank's internal audit program is normally expected to confirm that policies, procedures, and materials for the RAB activities have been properly approved by bank management and comply with laws, rules, and regulations. It ordinarily includes periodic on-site inspections of the partner as well as requires the partner to respond to and address issues identified by the internal audits. Examiners should also assess bank management's practices for conducting its own audits of the partner's processes, especially when the partner has not provided for appropriate audits. Examiners should verify whether internal audits assess how the program complies with applicable laws, regulations, and guidance and whether the internal audits are well-documented and readily available. Regulatory scrutiny and risk management expectations for certain practices will be greater for higher-risk portfolios and segments as well as for higher-risk partners.

Contingency Planning

Examiners should also direct their attention to arrangements for which all parties involved, including the bank, purchasers, servicers, and other affected parties, do not have proper contingency plans in place. The review should incorporate an assessment of how management normally reviews those types of plans, particularly for entities providing material services. The bank's plans normally involve transferring the program to another entity, funding the program internally, or shutting down the card program if the contract is terminated. Examiners should substantiate whether contingency plans are written and board-approved, identify specific actions the bank will take, and include appropriate information such as contact information for the parties involved. Concern is normally elevated when the plans only include activation after default has occurred and do not consider actions to be taken to lessen risk exposure as soon as indications of potential default by the partner have become apparent. For cases in which securitizations are used either by the bank, partner, or third party as the funding mechanism for the receivables, contingency planning takes on added elements of complexity. For example, the plan then needs to address the impact of potential events on the ability to continue to sell assets to the trust.

Comprehensive, well-thought out plans consider exposures in worst-case scenarios, such as the existing full open-to-buy exposure combined with the maximum time necessary to close accounts, as well as potential, more likely scenarios, such as those that consider the ability to reduce credit lines and close problem accounts. Without a sufficient contingency plan, the bank could find itself in a strained liquidity position, similar to an early-amortizing securitization.

Ability to Cease Authorizations

The ability to cease authorizations on the cards if the partner materially breaches the agreement or does not maintain adequate deposits, contingency reserves, or other required collateral is crucial. Contracts and cardholder agreements normally allow the bank to stop authorizations. If management does not have such authority with the processor, problems could arise. If a bank cannot shut down or limit authorizations in a timely manner, it increases its funding risk and may ultimately end up taking on credit risk that it may not be able to control. Even with the authority to cease authorizations, problems could arise regarding the Association membership, impacting the bank's aggregate risk position.

Risk Measurement Systems

Risk measurement systems to operate, monitor, and control issuing-RAB activities are critical components to the successful operation of such activities. Examiners should assess reports that management regularly receives to determine whether those reports enable management to gauge, in a timely and comprehensive manner, the risk posed by RAB activities. Management normally receives and reviews key management reports no less than monthly. The reports commonly include items such as the number and dollar volume of accounts, delinquency and charge-off volumes, over-limit data, customer service metrics, sales volumes, payment volumes, profitability, and any other relevant metrics needed to appropriately gauge risk. Concerns arise when appropriate segmentation methods are not incorporated and when management is not closely monitoring the trend and volume of available credit (open-to-buy) positions. The level of available credit coupled with normal or expected account usage can be an indicator of future potential settlement requirements. Reports reviewed by management also normally include information for measuring the partner's performance against that required by the contract. If securitization activities are associated with RAB activities, examiners should require that reporting on the securitization facilities and performance is incorporated. Monitoring the securitized pool by both the bank and the partner is particularly important when the partner relies heavily on securitization for funding. The bank could have to fund settlement if an early amortization is triggered. In addition, adverse impacts on the partner's financial wherewithal from poor performance in the securitized receivables could impact the partner's ability to cover its other assigned expenses, such as fines or cardholder reimbursements.

The level of detail and frequency of reporting funneled to the board is contingent on the size and risk profile of the operation in relation to the overall operations of the bank and its capital base. However, board reporting normally occurs no less frequently than quarterly and more frequently in certain instances, such as if concerns with the partner or portfolio are identified, if the arrangements involve higher-risk activities such as subprime lending, if the card portfolios involved are sizable compared to the bank's asset base and capital level, or if it is a new activity.

PARTNER'S OTHER RELATIONSHIPS WITH THE BANK

Concerns normally arise when management has not considered lending or other relationships that it has with the partner when analyzing the bank's total risk exposure or when each applicable area of the bank involved with the partner does not inform the other(s) about any adverse change in the partner's credit quality. For example, a partner's failure to make a loan payment likely points to emerging credit quality problems that may affect the partner's ability to meet settlement requirements or to fund the deposit and/or contingency reserve.

Lending to a partner essentially creates a conflict of interest that could result in management failing to take appropriate action against the partner when problems arise. For example, management might not want to discontinue marketing the card program because such an action might jeopardize repayment of the bank's loan to the partner. When management continues with a problem relationship, it often exacerbates the problems and increases subsequent losses. Examiners should look for evidence that management fully understands the total risk exposure when lending to a partner and carefully manages any such relationships to ensure any losses are minimized.

CAPITAL

A bank must hold appropriate capital for all of its business lines, including issuing-RAB arrangements. Effective policies limit the bank's volume of issuing-RAB activity relative to the bank's capital, the bank's risk profile, and management's ability to monitor and control the risks. Examiners assess the records supporting the capital allocation for issuing-RAB activities.

Existing regulations do not assess a specific capital charge for the aspects of issuing-RAB activities that the bank may be carrying off balance sheet. But, regulators may require the bank to hold capital above the regulatory minimums when appropriate. In general, factors considered in determining the proper level of capital to hold include:

- Quality of the partner, including reputation, experience, and organizational culture.
- Bank's management expertise in the area of credit card operations and RABs.
- Quality of the RAB oversight program.
- Profitability of the RAB activities from both the bank's perspective and the portfolio's perspective.
- Any instances of breach of contract.
- Deterioration in the partner's financial condition.
- Type of program offered through the RAB arrangement because certain types of business, such as subprime lending, are inherently riskier.
- Portfolio balance as well as open-to-buy trends and exposures.
- Quality and reasonableness of contingency plans.
- Audit findings.
- Bank's risk profile, including the adequacy of capital to support its other business lines.

Some RAB banks that are not holding the receivables consider risk-weightings similar to those that would be in place if the receivables were still on the bank's books, adjusted for collateral or other protection available. Examiners should expect that any methodology used will be well-supported and thoroughly documented and tie to considerations such as, but not limited to, those identified in the prior bullet points.

ACCOUNTING

As discussed, issuing RAB arrangements can have various structures. In some cases, the bank may have even been retaining the receivables for quite some time and only later decided to move the receivables off its balance sheet. Examiners will normally look at management's documentation of the RAB structure(s), including bookkeeping entries used. Because the structures, operations, and bookkeeping entries for the arrangements vary based on the governing contracts, accounting consequences also vary. All it would take to bring a receivable within the scope of FAS 140, *Accounting for Transfers and Servicing of Financial Assets and Extinguishments of Liabilities*, is for the receivable to be an asset of the bank for even a brief moment before being transferred to the partner or another party. In this case, management will need to determine whether or not the transfer of the receivables qualifies for sale accounting under FAS 140. To ensure all applicable accounting guidance (FAS 140 and otherwise) is followed, examiners would normally expect (and confirm) that management has consulted with the bank's accountants.

SUMMARY OF EXAMINATION GOALS – CREDIT CARD ISSUING RENT-A-BINS

Examiners must determine the extent of the bank's RAB activities as well as the level of risk that the activities pose to the bank. They must also determine whether the bank's capital level adequately covers the identified risk. Procedures for reviewing RAB arrangements are often similar to those procedures used to review other types of third-party arrangements. Examiners should review and assess:

- Applicable board and committee minutes, in coordination with the EIC.
- The bank's RAB policies to determine if they are comprehensive and that management is cognizant of the risks involved in such activities.

- Management's due diligence practices to determine whether this early line of defense against problematic relationships is effective.
- Staffing and resources to assess if the level is sufficient and qualifications are acceptable.
- The contract between the bank and the partner to determine if it is comprehensive and sufficiently limits the level of the risk that the bank assumes.
- Management's practices for testing and ensuring compliance with the contract to determine if emerging problems with the partner are promptly identified, thus allowing contract termination to be evoked timely when warranted.
- The marketing materials used for the program, including whether bank management exercises appropriate approval authority over such materials.
- The audit program to determine if it sufficiently encompasses issuing RAB activities.
- Deposit, contingency reserve, or other risk-mitigating funds/assets to determine if they are adequate, appropriately monitored, and readily available.
- Pricing structure and profitability data to assess whether fees received adequately compensate the bank and to identify any instances where portfolios might be unprofitable and, thus, appear to pose risk to both the partner and the bank.
- Contingency plans for thoroughness and reasonableness.
- Compliance with the AMG as well as any other applicable laws, regulations, or guidance.

In some cases, examiners should sample the partner's underwriting and other practices to compare them to established policies, laws, regulatory guidance, and other applicable devices. The use of or level of these types of review can be influenced by whether or not bank management is effectively reviewing and auditing such areas. If bank management is not properly reviewing the various areas, including underwriting and collections, then examination procedures will generally include expanded testing and review of the portfolio. Testing and portfolio review will also likely be expanded when higher-risk lending, such as subprime lending, or higher-risk partners are evident.

The following items might signal current or future elevated risk and warrant follow-up:

- Lack of appropriate RAB policies.
- Failure to appropriately monitor collateral protection, such as deposit and contingency reserve balances or other risk-mitigating devices.
- Unprofitable RAB operations.
- Unprofitable portfolios.
- Lawsuits or other complaints brought by cardholders.
- Compliance issues.
- Weak due diligence practices.
- Failure to properly monitor the partner's compliance with financial covenants and performance parameters.
- Failure to properly monitor performance of the portfolio.
- Failure to meet settlement requirements.
- Failure of the partner to provide open and timely communication with management.
- Weak understanding of the partner's activities and operations.
- Unfavorable correspondence from or to the Associations.

These lists are not exhaustive, and examiners must exercise discretion in determining the expanse and depth of review procedures to apply. If examiners identify significant concerns, they should expand procedures accordingly. In addition, examiners may limit the review as appropriate.

EXHIBIT D

XIX. MERCHANT PROCESSING

Merchant processing is the acceptance, processing, and settlement of payment transactions for merchants. A bank that contracts with (or acquires) merchants is called an acquiring bank, merchant bank, or acquirer. Acquiring banks sign up merchants to accept payment cards for the network and also arrange processing services for merchants. They can contract directly with the merchant or indirectly through agent banks or other third parties.

A bank can be both an issuing bank and an acquiring bank, but banks most often specialize in one function or the other. Merchant processing is a separate and distinct line of business from credit card issuing. It is generally an off-balance sheet activity with the exception of merchant reserves and settlement accounts, both of which are discussed later in this chapter. Merchant processing involves the gathering of sales information from the merchant, obtaining authorization for the transaction, collecting funds from the issuing bank, and reimbursing the merchant. It also involves charge-back processing. The vast majority of merchant transactions are electronically originated (as compared to paper-based) and come from credit card purchases at merchant locations or the point-of-sale (POS). Merchant processing increasingly includes transactions initiated via debit cards, smart cards, and electronic benefits transfer (EBT) products.

TRANSACTION PROCESS OVERVIEW

The payment networks are the center of the cardholder transaction process and maintain the flow of information and funds between issuing banks and acquiring banks. In a typical cardholder transaction, the transaction data first moves from the merchant to the acquiring bank (and through its **card processor**, if applicable), then to the Associations, and finally to the issuing bank (and through its card processor, if applicable). The issuing bank ultimately bills the cardholder for the amount of the sale. Clearing is the term used to refer to the successful transmission of the sales transaction data. At this point, no money has changed hands; rather, only financial liability has shifted. The merchant, however, needs to be paid for the sale. Settlement is the term used to refer to the exchange of the actual funds for the transaction and its associated fees. Funds to cover the transaction and pay the merchant flow in the opposite direction: from the issuing bank to the Associations, to the acquiring bank, and finally to the merchant. The merchant typically receives funds within a few days of the sales transaction.

In a simple form, the clearing and settlement processes for payments can be illustrated with a standard four-corners model (as discussed in the FFIEC IT Examination Handbook, Retail Payment Systems Handbook (March 2004)). In this model, there is a common set of participants for credit card payments: one in each corner (hence, the term four-corners model) and one in the middle of the diagram. The initiator of the payment (the consumer) is located in the upper left-hand corner, the recipient of the card payment (the merchant) is located in the upper right-hand corner, and the relationships of the consumer and the merchant to their banks (the issuing bank and the acquiring bank, respectively) reside in the bottom two corners. The payment networks that route the transactions between the banks, such as Visa, are in the middle of the chart. The information and funds flows for a typical credit card transaction are illustrated in a four-corners model[13] labeled Exhibit D on the next page. Information flows are presented as solid lines while funds flows are represented by dashed lines.

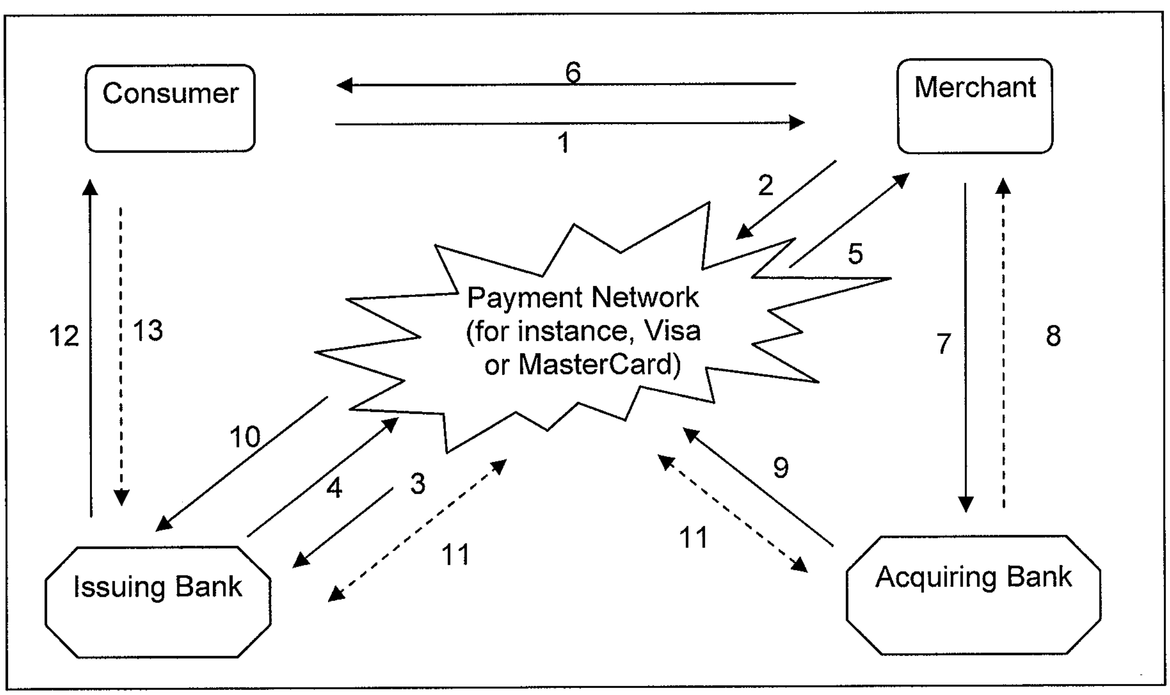
[13] The model and discussion generally mirror the model and discussion that is presented in the FFIEC IT Examination Handbook, Retail Payment Systems Handbook (March 2004).

Step 1:	The consumer pays a merchant with a credit card.
Steps 2 and 3:	The merchant then electronically transmits the data through the applicable Association's electronic network to the issuing bank for authorization.
Steps 4, 5, and 6:	If approved, the merchant receives authorization to capture the transaction, and the cardholder accepts liability, usually by signing the sales slip.
Steps 7 and 8:	The merchant receives payment, net of fees, by submitting the captured credit card transactions to its bank (the acquiring bank) in batches or at the end of the day[14].
Steps 9 and 10:	The acquiring bank forwards the sales draft data to the applicable Association, which in turn forwards the data to the issuing bank.

The Association determines each bank's net debit position. The Association's settlement financial institution coordinates issuing and acquiring settlement positions. Members with net debit positions (normally the issuing banks) send funds to the Association's settlement financial institution, which transmits owed funds to the receiving bank (generally the acquiring banks).

Step 11:	The settlement process takes place using a separate payment network such as **Fedwire**.
Step 12:	The issuing bank presents the transaction on the cardholder's next **billing statement**.
Step 13:	The cardholder pays the bank, either in full or via monthly payments.

Exhibit D



[14] Acquiring banks generally pay merchants by initiating Automated Clearing House (ACH) credits to deposit accounts at the merchants' local banks (possibly an agent bank). If an acquiring bank employs a third-party card processor, the card processor usually prepares the ACH file.

Exhibit D is only a simplistic example of the variety of arrangements that can exist. The parties for the transaction could be one of thousands of acquirers or issuers or one of millions of merchants and consumers. Further, there are many other ways the arrangements can be structured. For example, in on-us transactions, the acquiring bank and the issuing bank are the same. Also, the timing of the payment to the merchant (step 8 of Exhibit D) varies. Some acquiring banks pay select merchants prior to receiving funds from the issuing bank, thereby increasing the acquiring bank's credit and liquidity exposure. However, payment from the acquiring bank to the merchant often occurs shortly after the acquiring bank receives credit from the issuing bank.

The presence of third-party organizations coupled with the acquiring bank's ability to sub-license the entire merchant program, or part thereof, and the issuing bank's ability to sub-license the entire issuing program, or part thereof, to other entities also introduces complexities to the transaction and fund flows. For example, because the cost of technology infrastructure and the level of transaction volume are high for acquiring banks, most small acquiring banks rely on third-party card processors to perform the functions. In addition, issuing banks often use card processors to conduct several of their services. In intra-processor transactions, the same third party processes for both the acquiring bank and the issuing bank. Under the by-laws and operating rules/regulations of the Associations, the issuing banks and acquiring banks are responsible for the actions of their contracted third-parties, respectively.

A merchant submits sales transactions to its acquiring bank by one of two methods. Large merchants often have computer equipment that transmits transactions directly to the acquiring bank or its card processor. Smaller merchants usually submit transactions to a vendor that collects data from several merchants and then transmits transactions to the acquiring banks.

RISKS ASSOCIATED WITH MERCHANT PROCESSING

Some bankers do not understand merchant processing and its risks. Attracted to the business by the potential for increased fee income, they might underestimate the risk and not employ personnel with sufficient knowledge and expertise. They also might not devote sufficient resources to oversight or perform proper due diligence reviews of prospective third-parties. Many banks simply do not have the managerial expertise, resources, or infrastructure to safely engage in merchant processing outside their local market or to manage high sales volumes, high-risk merchants, or high charge-back levels. Many of a bank's risks may be interdependent with payment system operators and third parties. For example, the failure of any payment system participant to provide funding for settlement may precipitate liquidity or credit problems for other participants, regardless of whether they are party to payments to or from the failing participant.

For banks that engage in merchant programs or that are contemplating engaging in such programs, examiners should look for evidence that management understands the activity's risks which include credit, transaction, liquidity, compliance, strategic, and reputation risk. A failure by management to understand the risks and provide proper controls over such risks can be very problematic, and even lethal, to the bank. Take, for example, the case of National State Bank, Metropolis, Illinois. Inadequate control of the credit and transaction risks associated with its merchant processing activities contributed to a high volume of losses that ultimately depleted capital, threatened the bank's liquidity, and led to its closing by the Office of the Comptroller of the Currency (OCC) in December 2000.[15]

[15] As per press release PR-90-2000.

Credit Risk

A primary risk associated with merchant processing is credit risk. Even though the acquiring bank typically does not advance its own funds, processing credit card transactions is similar to extending credit because the acquiring bank is relying on the creditworthiness of the merchant to pay charge-backs. Charge-backs are a common element in the merchant processing business and are discussed in more detail later in this chapter. They can result from legitimate cardholder challenges, fraud, or the merchant's failure to follow established guidelines. Charge-backs become a credit exposure to the acquiring bank if the merchant is unable or unwilling to pay legitimate charge-backs. In that case the acquiring bank is obligated to honor the charge-back and pay the issuing bank which could result in significant loss to the acquiring bank. In a sense, the acquiring bank indemnifies a third party (in this case, the issuing bank that in turn indemnifies the cardholder) in the event that the merchant cannot or does not cover charge-back. Banks have been forced to cover large charge-backs when merchants have gone bankrupt or committed fraud. Acquiring banks control credit risk by using sound merchant approval processes and closely monitoring merchant activities.

Transaction Risk

Acquiring banks are faced with the transaction risk associated with service or product delivery because they process credit card transactions for their merchants daily. The risk can stem from a failure by the bank or any party participating in the transaction to process a transaction properly or to provide adequate controls. It can also stem from employee error or misconduct, a breakdown in the computer system, or a natural catastrophe. The acquiring bank needs an adequate number of knowledgeable staff, appropriate technology, comprehensive operating procedures, and effective contingency plans to carry out merchant processing efficiently and reliably. A sound internal control environment is also necessary to ensure compliance with the payment networks' rules. Formal reconciliation processes are also essential to limiting risk.

The high transaction and sales volume normally encountered with merchant processing programs creates significant transaction and liquidity risks. A failure anywhere in the process can have implications on the bank. Examples include an issuing bank's inability to fund settlement to the acquiring bank or a processing center's failure to transmit sales information to the issuing bank, thus resulting in a delay of or failure of funding to the merchant bank.

Liquidity Risk

Liquidity risk can be measured by the ability of the acquiring bank to timely transmit funds to the merchants. Acquiring banks often limit this risk by paying merchants after receiving credit from the issuing bank. If the acquiring bank pays the merchant prior to receiving credit from the issuing bank, the acquiring bank could sustain a loss if the issuing bank is unable or unwilling to pay. Some acquiring banks delay settlement and pay merchants one day after receiving the funds from the issuing bank. The delay allows the acquiring bank time to perform fraud reviews. For delayed settlement, which most commonly occurs when transactions are identified as suspicious or unusual, management is expected to have established formal procedures. Because merchant deposits can be volatile, risk may also arise if the acquiring bank becomes reliant on the merchant's deposits as a funding source for other bank activities. Furthermore, substantial charge-backs could potentially strain the bank's financial condition and/or reputation to such a degree that its creditors may withdraw availability of borrowing lines.

Associations guarantee settlement for transactions that pass through interchange. As a result, they may require collateral pledges/security if a bank's ability to fund settlement becomes questionable. This can create significant liquidity strains and potentially capital difficulties, depending on the size of the collateral requirement and/or the financial condition of the bank.

The Associations' rules allow them to assess the banks directly through the settlement accounts if the bank is not forthcoming with the collateral.

Compliance Risk

Compliance risk arises from failure to follow payment networks' rules and regulations, clearing and settlement rules, suspicious activity reporting requirements, and a myriad of other laws, regulations, and guidance. It can lead to fines, payment of damages, diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and lack of contract enforceability. Acquiring banks can limit compliance risk by ensuring a structured compliance management program is in place, the internal control environment is sound, and staff is knowledgeable. They can also limit risk by providing staff with access to legal representation to ensure accurate evaluation of items such as new product offerings, legal forms, laws and regulations, and contracts.

Strategic Risk

Strategic risk arises from adverse business decisions or improper implementation of those decisions. A failure by management to consider the bank's merchant processing activities in the context of its overall strategic planning is normally cause for concern. A decision to enter, maintain, or expand the merchant processing business without considering management's expertise and the bank's financial capacity is also normally cause for concern. Examiners should also pay close attention to how the acquiring bank plans to keep pace with technology changes and competitive forces. Examiners should look for evidence that the strategic planning process identifies the opportunities and risks of the merchant processing business; sets forth a plan for managing the line of business and controlling its risks; and considers the need for a comprehensive vendor management program. An evaluation of management's merchant processing expertise is critical to judging strategic risk. The bank's overall programs for audit and internal controls, risk management systems, outsourcing of services, and merchant program oversight are key to controlling the strategic risk.

Reputation Risk

Reputation risk arising from negative public opinion can affect a bank's ability to establish new relationships or services or to continue servicing existing relationships. This risk can expose the bank to litigation, financial loss, or damage to its public image. The bank's business decisions for marketing and pricing its merchant processing services can affect its reputation in the marketplace. Reputation risk is also associated with the bank's ability to fulfill contractual obligations to merchants and third parties. Most notably, the outsourcing of any part of the merchant processing business easily increases reputation risk. Decisions made by the acquiring bank or its third-parties can directly cause loss of merchant relationships, litigation, fines and penalties as well as charge-back losses. Concerns normally arise when the acquiring bank does not maintain strong processes for performing due diligence on prospective merchants and third-parties or perform ongoing evaluations of existing merchant and third-party relationships.

MANAGEMENT

Examiners should expect that management fully understand, prior to becoming involved in merchant processing and continuing thereafter, the risks involved and its own ability to effectively control those risks. Merchant programs are specialized programs that require management expertise, significant operational support, and rigorous risk-management systems. It can be a profitable line of business but, if not properly controlled, can result in significant risk to the bank.

Examiners should determine whether qualified management has been appointed to supervise merchant activities and to implement a risk management function that includes a merchant approval system and an ongoing merchant review program for monitoring credit quality and guarding against fraud. Bank staff's knowledge and skill-sets are expected to be commensurate with the risks being taken. For example, personnel responsible for processing charge-backs should have the technical knowledge and understanding of charge-back rules, and personnel responsible for approving merchant applications should have the ability to properly evaluate creditworthiness and identify high-risk merchants.

Examiners assessing risks of merchant programs should direct their attention to situations in which management has not put proper risk measurement systems in place to operate, monitor, and control the activity effectively. This includes situations that evidence the absence of regular management reports detailing pertinent information. Key reports generally include new merchant acquisitions, merchant account attrition, merchant portfolio composition, sales volumes, charge-back volumes and aging, fraud, and profitability analyses.

Examiner attention should be given to instances in which comprehensive, written merchant processing policies and procedures are absent or are not adequate for the size and complexity of operations. Necessary components of policies and procedures generally include:

- Clear lines of authority and responsibility (for example, the level of approval required to contract with certain types of merchants).
- Adequate and knowledgeable staff.
- Markets, merchant types, and risk levels the bank is and is not willing to accept.
- Limits on the individual and aggregate volume of merchant activity that correlates with the bank's capital structure, management expertise, and ability of operations to accommodate the volume (e.g., human and systems resources) as well as with merchants' risk profiles.
- Goals for portfolio mix and risk diversification, including limits on the volume of sales processed for higher-risk merchants and that take into account the level of management expertise.
- Merchant underwriting and approval criteria.
- Procedures for monitoring merchants, including financial capacity, charge-backs and fraud (regardless of who originates the merchants for the bank).
- Criteria for determining appropriate **holdback** or merchant reserve accounts.
- Procedures for settlement, processing **retrieval requests** and charge-backs, handling complaints, monitoring and reporting of fraud, and training personnel.
- Third-party risk management controls.
- Guidelines for accepting and monitoring agent banks.
- Guidelines for handling policy exceptions.
- MIS to keep management sufficiently informed of the condition of, and trends in, the merchant program.
- Audit coverage.

CAPITAL

Examiners should insist that the bank hold capital sufficient to protect against risks from its merchant business. In addition, they should determine whether management has established sound risk limits on the merchant processing volume based on the bank's capital structure, the risk profile of the merchant portfolio, and the ability of management to monitor and control the risks of merchant processing.

Associations limit the processing volume a bank can generate based upon the bank's capital structure, high-risk merchant concentrations, and charge-back rates. Banks operating outside the established thresholds (which may vary and are subject to change) are generally considered

to be high-risk acquiring banks by the applicable Association and may be subject to additional activity limits or collateral requirements.

No specific regulatory risk-based capital allocation(s) for merchant processing activities, which, as mentioned, are typically off-balance sheet, exist. Nevertheless, capital regulations permit examiners to require additional capital if needed to support the level of risk. Examiners frequently consider these measurements that take into account the volume of merchant activity:

- Risk Weighted Off-Balance Sheet Items for Merchant Processing = Average monthly merchant sales (Annual Merchant Sales/12) X 2.5 X 20 percent (conversion factor for off-balance sheet items) X 100 percent (risk weight category)[16].
- Tier 1 capital / (Average Total Assets + Risk Weighted Off-Balance Sheet Items for Merchant Activity).

MERCHANT UNDERWRITING

Evidence should corroborate that the bank scrutinizes prospective merchants with the same level of diligence used to properly evaluate prospective borrowers. Concerns may arise when the bank's underwriting does not consider the merchant's ability to cover projected charge-backs as well as its potential risk for fraud, high charge-back rates, and business failure. Merchant underwriting and approval policies generally:

- Define criteria for accepting merchants (for example, acceptable business types, time in business, location, sales and charge-back volumes, and financial capacity).
- Establish underwriting standards for the review of merchants.
- Define what information is required on the merchant application.
- Stipulate what information is required in the merchant agreement.
- Outline procedures and time frames for periodic review of existing relationships.

Merchant Review and Approval

Merchant underwriting provides an opportunity to reject a merchant that the acquiring bank determines has an unacceptable history of charge-back volumes, has a weak financial condition, is not operating a valid business, or is otherwise not acceptable for the bank's program. Limits for personnel approving new merchant accounts are usually based on the merchant's sales volume, and situations in which the designated bank personnel do not have appropriate levels of credit expertise in relation to that volume are cause for concern. Further, if the acquiring bank uses information collected by Independent Sales Organizations (ISOs) / Merchant Service Providers (MSPs), examiners should look for policies and controls to be in place for substantiating the quality of the information provided. In addition to exception guidelines and documentation requirements, underwriting standards generally include:

- A signed merchant application.
- A signed merchant processing agreement.
- A signed corporate resolution, if applicable.
- An on-site inspection report.
- Analysis of credit bureau reports on the principal(s) of the business.
- Evaluation of financial statements, tax returns and/or credit reports on the business.

---

[16] This calculation converts the off-balance sheet activity (merchant sales settled) to an on-balance sheet risk-weighted item. The 2.5 figure represents a 2.5 month average liability for charge-backs that is based on the premise that most charge-backs run off within 2.5 months. Technically, there is a potential 6 month window of charge-back liability. The 20 percent figure is the factor to convert the off balance sheet transactions subject to recourse to an on-balance sheet item. The 100 percent figure represents the risk weight applied based on capital regulations. The resulting risk weighted off-balance sheet items for merchant processing would be included in the denominator of the risk based capital ratios.

- Analysis of prior merchant activity, such as the latest monthly statements from the most recent processor.
- Analysis of projected sales activity (for instance, average ticket amount, daily/monthly sales volume).
- Assessment of any existing relationship (for example, a loan) with the bank.
- Consideration of the line of business and/or the product(s) offered by the merchant.
- Verification of trade and bank references.
- Evidence as to whether the merchant is on the Member Alert To Control High Risk Merchants (**MATCH**) system.

Principals:

Proper review by management normally includes conducting a background check on the business's principal(s), scrutinizing personal credit reports for derogatory information, and verifying addresses. Where appropriate and allowed by law, management may also perform a criminal background check.

MATCH:

Association regulations state that acquiring banks must check MATCH before approving a prospective merchant. The database contains a list of merchants that have been terminated for cause or that have made multiple applications for merchant accounts (because submitting applications to more than one acquiring bank simultaneously might indicate fraud). If an acquiring bank denies permission to accept cards to a merchant because of adverse processing behavior and fails to add it to the MATCH list, the acquiring bank can be liable for losses another provider might suffer from that merchant.[17]

If a merchant is listed on MATCH, management is expected to contact the listing bank regarding the termination reasons. MATCH status can help a bank determine whether to implement specific actions or conditions if a merchant is accepted. Examiners should pay attention to instances in which management has not carefully investigated a merchant listed on MATCH or in which their decision to accept or refuse a merchant has been solely based on the merchant being listed or not being listed on MATCH.

On-Site Inspection:

The goal of on-site inspections is to verify a merchant's legitimacy. The absence of documentation of the inspections, including photographs and a written inspection report normally is cause for concern as are situations in which the inspection was conducted by an individual who has a financial interest in its outcome. Acquiring banks signing merchants remotely sometimes find performing inspections themselves difficult or expensive. Often other acquiring banks or third parties will perform site inspections on an exchange or fee basis. In these cases, examiners need to assess whether management is well-informed of the other parties' inspection procedures and ensures that the procedures are, at a minimum, consistent with procedures management would use if conducting a proper inspection itself.

Products and Marketing:

The merchant's line of business and/or the products offered as well as its marketing practices are key factors for management to consider when it evaluates the credit quality of a merchant. The Associations segment merchants according to activity because the type of activity often is a good indicator of risk. Thus, it stands to reason that examiners may expect acquiring banks to

[17] According to the article entitled "Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box," authored by Ramon P. DeGennaro, and housed in the First Quarter 2006 edition of the *Economic Review* (Federal Reserve Bank of Atlanta).

continually analyze their merchant portfolios along similar guidelines. Acquiring banks typically compile a prohibited or restricted merchant list which includes the types of merchants they are unwilling to sign or are willing to sign only under certain circumstances.

While the extent of product and marketing evaluations varies, considerations normally include review of the merchant's business plans, merchandise, and marketing practices and materials (for example, catalogs, brochures, telemarketing scripts, and advertisements). In addition, shipping, billing, and return policies can be reviewed for unusual or inappropriate practices (for instance, customers being billed long before merchandise is shipped). These considerations can help determine, among other things, if: the business is of a type that typically has high charge-back rates; the merchant is selling a legitimate product; sales methods are legitimate and not deceptive; product quality and price are consistent with projected sales and charge-back rates; and customers will be satisfied with products ordered. Merchants offering low-quality products or services tend to incur more charge-backs, thus dissuading many banks from signing them.

The merchant's sales volume and time frame within which product delivery is completed are other considerations to evaluate risk. Generally, the greater the sales volume and the longer the time between transactions and product delivery, the greater the risk. For example, when a restaurant closes, an acquiring bank typically has less exposure to charge-backs for undelivered goods and services. In contrast, the failure of a travel agency could expose an acquiring bank to substantial charge-backs due to the high volume of reservations common in the travel agency business.

Certain types of merchant businesses can present increased risk. Although there are many reputable merchants whose sales transactions occur without a credit card being present (card-not-present merchants), these merchants generally present higher charge-back risks for acquiring banks. In particular, mail order and telemarketing (MO/TO) merchants and adult entertainment services merchants, in aggregate, tend to display elevated incidents of charge-backs. Merchants without an established storefront (for example, door-to-door salesman and flea market vendors) also typically pose greater risk for charge-backs. The risk of charge-back is also higher if the merchant sells products for **future/delayed delivery**, such as airline tickets, health club memberships, travel clubs, or internet purchases. The increased risk associated with future delivery of products results, in part, because customer disputes are normally not triggered until the date of delivery. High charge-back rates are also generally associated with certain selling methods, such as sales pitches involving gifts, cash prizes, sweepstakes, installment payments, multi-level marketing, and automatic renewals unless the consumer opts out. Association regulations define certain broad business categories as high-risk merchants. These categories in general present higher risk, but each individual merchant in the category may not necessarily be high risk. Appropriate procedures and risk controls for high-risk merchants generally include:

- Criteria for determining the types of merchants the bank is or is not willing to sign and under what circumstances.
- Increased emphasis on underwriting considerations regarding products and marketing in evaluating the merchants.
- Limitations on the volume of high-risk merchant transactions processed relative to the bank's total merchant portfolio.
- Criteria for determining the appropriate level of holdback or reserve accounts to sufficiently cover the level of credit risk.
- Appropriate pricing of these merchants in relation to the charge-back risk and any costs associated with increased monitoring.
- Heightened monitoring and problem resolution. For example, for charge-back monitoring, banks may set lower charge-back thresholds for required remedial action and/or a shorter timeline for problem resolution for those merchants exceeding acceptable charge-back thresholds.
- Compliance with bankcard regulations regarding registration of certain high-risk merchants and assigning proper **Merchant Category Codes (MCC)** to merchants.

Merchant Agreements

If management has not sought legal advice when developing merchant agreements and/or referred to network guidelines for contracting, closer scrutiny of such agreements may be warranted. Typical contents of a merchant agreement include but are not limited to:

- Fees and pricing.
- Merchant requirements at POS.
- Requirements for cardholder information security.
- Prohibition of **split sales drafts** and **laundering** of sales drafts.
- Merchant liability (for example, charge-backs and reserves).
- Notification of ownership changes or substantive marketing and product changes.
- Right to hold funds (for example, bank's right to freeze deposits when fraudulent activity suspected).
- Termination provisions.
- Internet provisions (for example, encryption and web-site displays).

Periodic Review

Concerns normally become elevated when management is not monitoring the financial condition of high-volume and high-risk merchants on an ongoing basis and/or when the bank's policy has not addressed the frequency of reviews and the size of merchants requiring reviews. Examiners should assess management's practices for considering volume, concentrations, high-risk industries, and charge-back history in establishing the thresholds for periodic reviews. Depending on the composition of the bank's merchant portfolio, examiners may not necessarily expect the bank to conduct credit reviews of smaller merchants on an ongoing basis if the bank used sound underwriting guidelines at acquisition and if the bank is using strong controls to monitor all merchant transactions, including fraud and charge-back monitoring. Examiners might observe cases in which databases (for items such as risk scores and bankruptcy filings) are used to periodically screen the merchant portfolio.

Communication between merchant program and loan personnel regarding changes in the merchant's credit quality is key part of assessing any shared banking relationships. For example, an unacceptable charge-back rate for a merchant might indicate emerging credit quality problems that could trigger the need to review any lending relationships with the merchant. Likewise, concerns that identify merchants as problem borrowers could trigger the need to review merchant arrangements. If credit information shows deterioration in the merchant's financial condition, the bank may want to reduce its risk exposure from merchant processing. For instance, when dealing with a financially-unstable merchant, the bank might require a holdback or security deposit, as discussed later in this chapter.

Internet Merchants

The lower level of barriers encountered when setting up an Internet merchant increases the risk of fraudulent businesses or businesses with minimal financial resources being established compared to the risks associated with traditional merchants. This risk elevates the need for acquiring banks to conduct thorough underwriting reviews of internet merchants. Whether fraud and charge-back risks warrant additional risk-mitigation techniques, such as delaying settlement or setting up reserves, is a critical decision that normally occurs during the underwriting process.

Electronic commerce via the Internet poses additional privacy and security concerns. The absence of or weak transaction and data security controls for customer transactions and storage of customer information are cause for concern. Secured servers and data encryption technologies help to protect data and transaction integrity. Other items considered normally include whether the merchant meets the following general web site display guidelines:

- Description of goods and services offered.
- Customer service number.
- Company's e-mail address.
- Statement regarding security controls.
- Delivery methods and timing.
- Refund and return policies.
- Privacy statements (permissible uses of customer information).

PRICING

One of the key aspects of a successful merchant program is appropriately setting the fees that the merchant will be charged for sales transactions and acquiring bank services. Merchant pricing is extremely competitive, especially for large- and national-scale merchants who generate high transaction volumes. High transaction volumes can lead to economies of scale and possibly increased income. Examiner should look for evidence that banks have adopted a pricing policy that outlines the methods used for pricing, authority levels, and repricing procedures. A pricing policy can facilitate consistency in pricing practices and help optimize profit margins.

Acquiring banks use various methods to price merchants. Smaller merchants are frequently priced with a single discount rate based on merchant volume and average ticket size. Acquiring banks frequently use unbundled pricing for medium to large merchants. Unbundled pricing is the method of assigning fees for the cost of each service used. Examples of unbundled services include interchange, authorizations, and charge-backs. Other fees may include, but are not limited to: statement preparation, application, customer service, membership, maintenance, and penalty fees (for example, for violating payment network rules).

Examiners should evaluate the bank's practices for ensuring that pricing is consistent with the risk posed by the merchant. Acquiring banks sometimes use a pricing model to determine the target discount rate. They might maintain one or more pricing models, with model usage driven by the merchant's sales volume and/or industry classification. Pricing models allow the acquiring bank to quickly substitute variables regarding sales volumes, average ticket size, revenues and expenses to produce a projected profit margin. A failure of the pricing model to include all direct and indirect expenses may render the model's results meaningless. A model's accuracy depends upon the reasonableness of the assumptions used.

Pricing Components

Discount Rate:

Acquiring banks assign a discount rate for each merchant when the merchant agreement is signed. The discount rate is the percentage that gets "discounted" off the transaction amount that is paid to the merchant, hence the term discount rate. In a simple case, the discount represents a single rate charged to a merchant based on the merchant's sales volume. For example, a merchant with a 2 percent discount rate receives $98 for a $100 credit card sale. Most merchant agreements allow the acquiring bank to change the discount rate for various cost increases. Numerous factors influence the discount rate charged, including, but not limited to, the transaction method, processing volume, and type of merchant business. For example, merchants who use **electronic data capture (EDC)** are typically charged lower discount rates than paper-based merchants. Discount rates generally range from 1 to 4 percent for small to medium-size merchants and sometimes well below that range for large-volume merchants.

When considering the range of discount rates used by the bank, examiners should call on management to readily explain outliers, including those that are well below the normal range. Banks sometimes give merchants a favorable discount rate because of existing commercial loan

or deposit relationships. In other cases, the discount rate is favorable due to a credit card equipment lease arrangement. Packaging may be an acceptable practice, but does not eliminate the need to measure the overall profitability of a merchant relationship. Further, examiner attention should be drawn to situations in which management has offered favorable discount rates to insiders or their related interests.

Interchange Fees:

Interchange fees represent compensation paid by the acquiring bank to the issuing bank. Thus, they are recorded as an expense on the acquiring bank's income statement and as a revenue source on the issuing bank's income statement. Interchange fees are based on several factors such as volume, size, and type of transaction and are usually set by the Associations. They average less than two percent of the purchase price and are typically one of many considerations in determining the size of the discount rate that the acquiring bank charges the merchants. (For on-us transactions, interchange may be reduced, if not entirely eliminated.) A number of merchants and merchant groups have filed lawsuits alleging that the interchange fees set by the Associations for credit card transactions violate anti-trust laws and that the fees paid to accept payment cards are too high. In last quarter of 2006 the Associations began offering pubic access to interchange rate information.

Processing Fees:

Processing fees cover the costs associated with data processing services and vary depending on the size and number of transactions the merchant submits per batch. The processing fee may include data capture and authorization costs. It might go directly to the bank if it handles the processing or to the bank's third-party processor.

ISO/MSP Fees:

The ISO/MSP fee is the amount the acquiring bank pays the ISO/MSP for services provided. It is negotiated and often represents a percentage of the volume that the ISO/MSP-sponsored merchants bring to the bank. The fee agreement between the bank and the ISO/MSP is normally considered when pricing merchants obtained through an ISO/MSP.

Agent Bank Commission:

The agent commission is a fee passed to the agent bank for signing a merchant. This fee could be built into the discount rate or be assessed separately.

Other Income:

Acquiring banks sometimes offer other programs to generate fee income (for instance, equipment leasing). Instances in which management has not researched the legal and compliance aspects of products or services offered or has not priced the programs adequately warrant scrutiny.

Monitoring Pricing

Examiners should evaluate management's practices for ensuring that merchants are priced appropriately throughout the life of the contract. Best practices by management may include verifying actual volumes and ticket sizes after signing a new merchant (for example, at six months into the relationship) to ensure consistency with volumes and ticket sizes anticipated. Examiners should assess management's practices for ensuring the discount rate is in line with the application estimate and original pricing model assumptions. In general, a failure by management to review all significant merchants for repricing at least annually elevates concern. Further, if any merchants are or have been unprofitable, examiners should accordingly inspect management's repricing practices for those merchants. Merchant agreements typically allow

acquiring banks to increase pricing at any time during the contract's life.

Profitability Analysis

Merchant programs can be profitable. Although competition with third-party processors has lowered margins, banks have been able to compete due to their strong marketplace presence. Banks are able to generate new merchant accounts through their branch networks and existing customer relationships.

Merchant processing is characterized as a high transaction volume, low profit margin business. Only efficiently run departments with strong cost controls can operate profitably. Examiners should analyze profitability reports used by the bank to measure the profitability of the merchant processing operations to determine if it is consistent with the size and complexity of the operations. Reports should detail key performance measures such as net income to sales and net income per item. Ideally, it should be able to segment profitability by merchant, acquisition channel, and industry.

Examiners should normally expect profitability analyses for merchant operations to be distinctly separate from the analyses of other banking activities and to include all direct and indirect costs. Direct costs include costs such as those for internal data processing, merchant accounting, fraud and charge-back losses, personnel, and occupancy. Indirect costs may include corporate overhead expenses such as those for human resources, legal, and audit services. The level of detail and frequency of board reporting is contingent on the size of the operation in relation to the overall operations of the bank and its capital base.

FRAUD MONITORING

Management's ability to quickly detect fraudulent activity is important in controlling losses. The merchant, then its acquiring bank, are the parties liable for certain types of losses. Persons possessing stolen credit cards sometimes take advantage of unsuspecting store clerks, or merchants sometimes perpetrate fraud. Merchant fraud can be extremely costly if not discovered quickly. Examples of merchant fraud include **factoring** and draft laundering. New merchant accounts are particularly susceptible to fraud such as **bust-out scams**. Examiners should insist that banks have a fraud detection system to identify and monitor potentially fraudulent activity.

Fraud Detection Methods

Fraud identification that relies exclusively on excess charge-back activity analysis is normally cause for concern because there are a number of other indicators that can point to fraud. A primary tool used by management for fraud detection is an exception report that details variances from a multitude of parameters established at account set-up. Along with charge-backs, basic parameters usually include daily sales volume, average ticket size, multiple purchases of the same dollar amount, multiple use of the same cardholder number, percentage of keyed versus swiped transactions (because keyed transactions frequently are associated with card-not-present transactions which are normally higher-risk), number of authorizations declined, authorizations during non-business hours, and high volume of authorizations in relation to transactions. A daily exception report lists merchants that are outside of any of the parameters.

Most large-volume processors have established exception parameters based on industry or merchant type. Examiners should review management's practices for periodically updating parameters. For example, management might set the daily sales threshold at a percent of a prior timeframe's activity (for instance, 110 percent of the three months' average). The margin allows for normal growth of the merchant and compensates for seasonal sales patterns.

Some banks use neural network technologies for fraud detection. These complex computer programs can compare each transaction against the merchant's prior sales patterns. Though more sophisticated than a traditional exception report, smaller merchant processors may be unwilling or unable to purchase these technologies on an ongoing basis. Instead, some acquiring banks selectively route higher-risk transactions through a neural network while confining the remainder of transactions to exception reporting.

Some banks also use Informational databases (such as those for scoring, bankruptcy, trade, and fraud) to identify at-risk merchants. Merchants that have financial or legal difficulties often have a higher propensity to falsify transactions.

Associations provide educational materials to acquiring banks and merchants about the industry's latest fraud detection techniques. They also prepare fraudulent activity reports for each acquiring bank. The reports are not intended to replace the bank's own fraud system. Rather, examiners should expect to see that such reports supplement the internal system. Certain circumstances require management to document its plan to correct a merchant's unacceptable sales practices.

Inactive merchant accounts can signal potential fraud. For example, inactivity could signal a bust-out scam wherein a fraudulent merchant signs with several acquiring banks simultaneously, moving from one to the next as the scam is perpetrated or detected. When exception reports flag an inactive account, management normally follows up with the business owner.

Other potential warning signs of fraud generally include:

- Evidence that credit card purchases have been intentionally structured by a merchant to keep individual amounts below the "floor limit" to avoid approval requirements.
- Merchant account activity that reflects a substantial increase in the number and/or size of charge-backs.
- Merchant's deposit of sales drafts made payable to a business or businesses other than the business named on the account.
- Merchant's frequent request that funds be wire transferred from the merchant account to other institutions in other parts of the country or to offshore institutions almost immediately after deposits are made.
- Merchant that is engaged in telemarketing activities and is the subject of frequent customer complaints.
- Merchant account deposits that appear to exceed the level of customer activity observed at the merchant's place of business.
- Merchant that has access to electronic data capture equipment but frequently inputs credit card account numbers manually (for example, if manually keyed transactions exceed 10 percent of total transactions).
- Merchant that has a sudden or unexplained increase in the level of authorization requests from a particular merchant location.

Fraud Investigations

Examiners must expect management to take swift action when it encounters suspicious transactions or other suspicious activity. Management's investigation may include verifying purchases with the issuing bank and/or obtaining copies of paper-based transaction tickets from the merchant. An acquiring bank's quick response will help minimize losses to it and the issuer as well as provide timely information to law enforcement agencies. Changes in a merchant's business operations such as changes in ownership, business principals, bank accounts, merchandise, sales methods, or target market normally also warrant an investigation.

Merchant agreements normally allow the acquiring bank to delay settlement until questionable transactions are resolved. Once fraud is suspected, management must follow Suspicious Activity Report (SAR) guidelines. Examiners should evaluate the bank's processes for terminating fraudulent merchant accounts and placing such merchants on MATCH. They should also consider the acquiring bank's and its processor's practices for suspending or blocking settlement and authorization processing to a terminated merchant's account. Such procedures are intended to prevent further deposits and **account testing**.

CHARGE-BACK PROCESSING

Credit risk arising from charge-backs is an acquiring bank's primary risk and can result in significant financial loss. If a merchant is unable to pay its charge-backs, the acquiring bank must pay the issuing bank. Large charge-back losses can also result from deliberate fraud undertaken by the merchant. For example, a merchant might sell deceptive or misleading merchandise or never deliver the product. Authorization issues, inaccurate or incomplete transaction information, and processing errors can also result in charge-backs. Charge-backs are governed by a complex set of rules and time limits that can be costly to merchants and acquiring banks if disregarded. Charge-back losses realized by the bank are listed as other non-interest expense on the Call Report.

The most effective preventive measure against charge-back losses is thorough underwriting prior to merchant acceptance. Nonetheless, examiners should expect that an acquiring bank have strong controls in place to accurately and timely process charge-backs and retrieval requests. The bank may lose a charge-back dispute (thus resulting in a loss) if it does not adhere to charge-back rules. The absence of effective charge-back monitoring to identify problem merchants for remedial action normally draws examiner attention. Quickly considering problem merchants for termination may help avoid or limit loss.

Charge-Back Transaction Flow

Cardholders initiate charge-backs, for instance when they are dissatisfied with the product, did not receive the merchandise or service, or did not authorize the charge. A consumer first tries to resolve the dispute with the merchant. If unsuccessful, the consumer informs the issuing bank about the dispute, and the issuing bank posts a temporary credit to the cardholder's account. The issuing bank then requests documentation from the merchant to authenticate the transaction and possibly resolve the dispute. If the dispute is upheld, the amount is charged back to the merchant's account and the consumer does not pay for the disputed charge. The consumer has 60 days from the day he or she receives the statement to report a dispute to the issuing bank.

Issuing banks can also initiate charge-backs when the merchant does not follow proper card acceptance and authorization procedures or when there is a problem with the credit card account (for example, it is not valid or has been terminated). The acquiring bank's contingent charge-back liability generally spans 90 to 120 days (but up to 180 days for certain transactions).

Associations have strict charge-back processing regulations. For example, charge-backs occur when a merchant fails to provide copies of requested sales tickets. If the merchant does not fulfill retrieval requests within prescribed time frames, it loses the charge-back dispute. Merchants must also follow other card acceptance procedures, including obtaining authorizations, as depicted in the governing documents.

Charge-Back Monitoring

The Associations notify acquiring banks about high charge-back merchants. Once management has received notification of excessive charge-back activity, examiners should expect management to promptly take appropriate steps to bring charge-back rates down to acceptable

levels. The steps may include, but are not limited to, reviewing procedures with merchants or developing a detailed and comprehensive charge-back reduction plan. If the charge-back volume is not sufficiently reduced within established timeframes, the Associations may impose substantial fines against the acquiring bank.

Although the Associations notify acquiring banks about merchants with excessive levels of charge-backs, examiners normally have concern when an acquiring bank's own risk management practices do not detect such merchants or when charge-back processing staff is not alert for merchants with excessive retrieval requests or charge-backs. Numerous charge-backs could indicate an unscrupulous merchant or a need for additional training.

Risk Mitigation for Charge-Backs

Acquiring banks often establish specific merchant reserve accounts, or holdback reserves, for higher-risk or high-charge-back merchants. Holdback reserves are also used to limit a bank's credit risk when the merchant's product or service involves future/delayed delivery. They are funded by a lump sum payment or by withholding part of each day's proceeds. Examiner should expect these types of specific reserve accounts to be adequately funded.

The acquiring bank might also fund a general allowance account, similar to the ALLL (although not commingled therewith), for a portfolio of merchant accounts. The method used to determine the allowance allocation varies but is typically based on contingent charge-back exposure for the entire portfolio. Such an allowance is reported as an "other liability." Examiners should analyze management's merchant reserving methods to determine whether these types of allowances are sufficiently funded.

An acquiring bank might also obtain merchant charge-back insurance which is intended to provide protection against uncollectible charge-backs. While insurance products potentially provide some level of protection, they are not a substitute for strong risk management practices. Insurance contracts frequently include significant limitations or restricting clauses that constrain the usefulness of the contract in the event of an actual loss (for instance, limits on types of losses covered and restrictions based upon bank management's action or inaction in managing the merchant portfolio). In addition, the insurance carrier might not have the financial ability to fund the contract in the event of significant loss.

Larger merchant processors employ collectors to recover charge-back losses and other fees. A collector seeks remedy from the principals of the business through negotiations or civil action.

Accounting for Charge-Backs

Management is expected to appropriately detail charge-back losses on Call Reports as other non-interest expense and reverse any uncollectible fees from income in a timely manner. Any collected funds are to be reported as other non-interest income.

ACQUIRING RENT-A-BINS

A BIN[18] is a number assigned by an Association to identify the bank for authorization, clearing, settlement, card issuing, or other processes. Ownership and usage of BINs can result in significant credit risk exposure if not appropriately controlled, especially when the acquiring bank owns a BIN and permits other entities to share in the usage, otherwise known as an acquiring Rent-a-BIN. The concept of Rent-a-BINs (RAB) was introduced earlier in this manual. There are

[18] An ICA number, which is similar to a Visa BIN, is assigned by MasterCard. ICAs and BINs are collectively referred to as BINs in this manual. Examiners may also encounter arrangements with American Express and Discover, particularly now that their access to banks has expanded.

issuing RABs and acquiring RABs. Issuing RABs were the focus of the Credit Card Issuing Rent-a-BINs chapter while acquiring RABs are discussed here.

Acquiring RABs draw their names from the characteristic of acquiring merchant contracts and cardholder transactions. Under an acquiring RAB arrangement, an acquiring bank permits ISO/MSPs to use the bank's BIN(s) to acquire merchants and settle their credit card transactions. The ISO/MSP retains the majority of income, and the BIN-owner receives a fee for the use of its BIN(s). Although it has minimal operational involvement, the BIN-owner has primary responsibility to the Association if any user fails to perform. The BIN-owner retains the risk of loss as well as responsibility for settlement with the Associations consistent with the contract between the bank and the Association. Thus, examiners should insist that management rigorously oversee and control acquiring RAB arrangements to ensure that the ISO/MSP is appropriately managing the risks. Oversight controls are important, even if the ISO/MSP shares liability with the bank. A failure by management to consider any lending relationships the bank has with ISO/MSPs in analyzing total risk exposure warrants examiner attention. Given the substantial risk involved, many banks are reluctant to enter into acquiring RAB arrangements.

Risk also exists when an acquiring bank uses a BIN owned by another bank. If the BIN-owning bank fails to perform, the Associations may hold all of the BIN-users liable. RABs require close examiner analysis of the acquiring bank's program to determine the extent of risk to the bank.

THIRD PARTIES

The success of a payment system depends on the credit quality of its participants and its operational reliability. As mentioned, the presence of third parties coupled with the bank's ability to sub-license the entire merchant program, or part thereof, to other entities, introduces numerous complexities in the transaction and funds flows related to credit card transactions. Third parties such as ISO/MSPs and servicers are used by acquiring banks for a variety of functions like soliciting merchants, merchant application processing, charge-back processing, fraud detection, customer service, accounting services, selling/leasing electronic terminals to merchants, transaction processing, authorizations, and data capture. Each acquiring bank's program is unique regarding the number of third parties used and the services provided. Examiners should require that banks have proper risk management policies and procedures to control the applicable third-party risks.

An acquiring bank, as the Association member, is ultimately responsible for the settlement of transactions processed through its BINs, regardless of the third parties used and the contents of its contracts with those parties. The acquiring bank (BIN-owner) needs to take an active role in ensuring the quality and integrity of the services these third parties provide because the quality of services among third parties varies greatly. Examiners should pay close attention to instances in which the bank relies on the guarantee of a third party against losses as a substitute for prudent risk management. Losses associated with high-risk or fraudulent credit card activity can be substantial and easily reach figures well beyond the means of a seemingly financially capable third party. Banks have incurred significant losses from failing to control third-party activities. Uncontrolled growth, fraud, and inadequate operations by the third parties have all resulted in significant problems for banks. ISO/MSPs in particular could be motivated by their own profits at the expense of merchant portfolio quality and often have limited financial capacity.

Regardless of the third parties used and any guarantees provided, the examination approach requires that bank staff have the expertise and knowledge of the business to properly manage the risks and that management have a sound plan for managing its merchant program as well as policies and procedures in place to control the risks associated with using third parties and to properly limit the use of the bank's BINs by others. For instance, the final review of merchant applications and the decision to approve or decline a new account should be controlled by the BIN-owner.

The examination should verify that the bank's policies and procedures, in general, provide for:

- A due diligence process to: determine the third party's character and ability to perform the services; assess the risks associated with using the third party; and establish risk controls.
- A process for ensuring the adequacy of written agreements.
- A monitoring process for the third party's operations and financial condition.

Examiners should look for evidence that due diligence processes, in general, include:

- Determining that the third party has the operational and financial ability as well as expertise to perform the services.
- Performing thorough background checks on the third party's principals and key individuals to determine their good standing, including bank and trade references, credit reports, and, where appropriate, criminal backgrounds.
- Analyzing the financial capacity of the third party and its principals to determine continued viability and capacity to absorb losses.
- Performing an on-site inspection.
- Assessing the third party's marketing practices and the types of merchants targeted.
- Assessing the risks associated with the use of the third party and the controls needed to manage the risk (for example, underwriting standards, security of sensitive information, reporting requirements, and procedures for settlement, charge-back processing, fraud monitoring, and pricing).
- Establishing criteria for requiring additional loss controls, such as reserves or security deposits to absorb losses stemming from merchant fraud and charge-backs.
- Ensuring separation of duties for activities performed (for example, the individual conducting the on-site inspection should have no financial interest in its outcome).
- Registering third parties with Associations as required.

The examination should also include assessing whether the bank's monitoring process, in general, includes:

- Periodically reviewing the financial condition of third parties and their principals to determine capacity to meet commitments and remain in good standing.
- Reviewing allowances to ensure they are consistent with the condition of the third party and volume of business generated.
- Reviewing compliance with the bank's established requirements (for example, underwriting standards, settlement and charge-back processing, fraud monitoring, merchant pricing, and security of cardholder information).
- Periodically conducting on-site inspections.
- Periodically evaluating the third party's internal controls (for example, through review of operational audits).
- Assessing system audits for third parties performing processing tasks.
- Periodically reviewing marketing practices.
- Reviewing contingency plans to assure continuity of operations.
- Documenting the bank's relationship with the third party.
- Checking compliance with contractual provisions.
- Determining the adequacy of the bank's controls over third party access to sensitive information.

Contractual Considerations

Concerns arise when management has not obtained a signed, written agreement between it and each third party or when the agreement fails to take into consideration business requirements, key risk factors identified during the due diligence process, and the Associations' regulations. Legal counsel familiar with merchant processing normally reviews contracts prior to signing.

Contractual considerations generally include:

- Responsibilities of each party.
- Terms specifying compensation, payment arrangements, price changes, and time frames.
- Provisions prohibiting the third party from assigning the agreement to any other party.
- Frequency and means of communication and monitoring activities of each party.
- Provisions regarding the ownership, confidentiality, and non-disclosure of cardholder information as well as compliance with cardholder information security standards.
- Recordkeeping requirements and whether each party has access to these records.
- Responsibility for audits, the bank's access to those audits, and whether the acquiring bank has the right to perform an audit of the third party.
- Notification requirements of system changes that could affect procedures and reports.
- Type and frequency of financial information the third party will provide.
- Termination parameters, including potential penalty provisions.
- Maintenance of an adequate contingency plan by the third party.

Additional contractual considerations for ISO/MSPs generally include:

- Tying compensation to the merchant portfolio's performance (for instance, charge-back activity).
- Defining responsibilities for fraud and charge-back processing and losses.
- Requiring security deposits from the ISO/MSP, particularly if its financial condition is weak or the quality of the merchants it solicits presents significant risk.
- Establishing remedies to protect the bank if the ISO/MSP fails to perform (for example, indemnity provisions, early termination rights, and delayed payment).
- Providing criteria for acceptability of merchants.
- Specifying that the bank owns the merchant relationships.
- Controlling the future use and solicitation of merchants.
- Defining the allowable use of the name and logo of the bank and the ISO/MSP.
- Permitting bank employees to conduct onsite inspections of the ISO/MSP.
- Specifying that all applicable regulations and Association rules are to be followed.

Association Requirements Regarding Third Parties

The bank's risk management program needs to consider the Associations' requirements regarding third parties. Each acquiring bank is expected to register third parties according to the Associations' guidelines before accepting services. Associations generally require an initial registration fee and annual fees for each third party under contract. The fees are normally passed on to the third party.

The Associations have specific guidelines relating to contract provisions, functions controlled by the acquiring bank, accessibility of procedural audits, and recordkeeping requirements. In particular, Association regulations state that:

- All new merchant accounts should be reviewed with final approval controlled by the acquiring bank.
- A registered third party cannot subcontract its bankcard-related services to another business. Bankcard-related services can only be provided by businesses with a direct written contract with an Association member.
- All aspects of a member's relationship with a third party should be documented.
- Members are responsible for ensuring that merchants receive payment for the card transactions deposited.

Even after registration, the acquiring bank remains responsible for ensuring compliance with the Associations' operating regulations. The regulations make the acquiring bank liable to the Associations for the actions of third parties. Banks are to periodically submit certain information on third parties used to the Associations and can be fined by the Associations for not doing so.

Agent Banks

Agent banks contract with merchants on behalf of an acquiring bank. Agent banks are typically community banks that want to offer merchant processing services to their merchant customers but that do not have the management expertise and/or do not want to invest in the infrastructure needed to serve as an acquiring bank. Acquiring banks generally provide backroom operations to the agent bank. Depending upon the contractual arrangement, the agent bank may or may not be liable to the acquiring bank in the event of charge-back or fraud losses. Agent banks with liability typically perform merchant underwriting. Agent banks without liability are typically called referral banks. In a referral arrangement, the acquiring bank performs the underwriting, executes the merchant agreement, and accepts responsibility for merchant losses. Acquiring banks sometimes compensate the referral bank byway of a referral fee.

If examining an agent bank, examiners should determine whether management fully understands the bank's financial liability for charge-backs as well as its responsibilities under the agreement with the acquiring bank. An agent bank should have appropriate procedures in place to ensure it fulfills its obligations under such agreement. Examiners should expect that agent banks with liability have proper risk management policies and controls in place for merchant underwriting and monitoring, pricing and profitability, and third-party relationships.

Examiners should determine whether management of an agent bank has ensured underwriting guidelines meet the acquiring bank's underwriting standards, at a minimum, and represent an appropriate level of risk for the agent bank to hold. Acquiring banks may decline a merchant if it poses undue risk or does not meet the bank's minimum standards. Other agent bank tasks include performing ongoing monitoring of sales, charge-backs, and fraud.

Examiners should look for evidence that pricing of agent relationships is sufficient to cover costs, including any fees paid to the acquiring bank and anticipated losses. Depending on the size of the agent bank's merchant portfolio, separate profitability reports on this business line may not be necessary. But, that does not negate management's responsibility to determine if the service is profitable to the bank. If profits are minimal or nonexistent, considerations would include whether the risk is sufficiently offset by the intangible benefits gained from offering the services.

Examiners should expect to see a written agreement clearly outlines both agent and acquiring banks' responsibilities. They should also determine whether the agent bank has performed appropriate due diligence regarding the acquiring bank's ability to meet its obligations under the contract and, similarly, whether acquiring banks have put appropriate controls in place regarding the use of agent banks. Examiners should evaluate controls for maintaining appropriate underwriting standards and processing volumes and for monitoring the agent's financial condition and processing volume. Instances in which the financial condition is not consistent with its merchant portfolio risk profile and/or the activity's volume normally raise concern.

Loans to Third-Party Organizations

Examiners should pay attention to situations in which management has failed to fully understand the total risk exposure when lending to third parties that perform services for the bank, including for its merchant program. The lending relationship creates a potential conflict of interest and increases the bank's overall credit risk. The risk exposure is not only the loan(s) to the third-party but also the contingent liability from merchant processing activities by the third party conducted through the bank's BIN. Lending to a third-party organization sometimes results in management failing to take appropriate action against the third party when problems are identified. For example, management may not want to stop processing for the ISO/MSP because it may jeopardize repayment of the bank's loan. As a result, management could continue with a problem relationship, which may increase the problems and subsequent losses. Examiners should evaluate management's processes to determine and control total risk exposure.

Contingency Planning

Concerns also surface when acquiring banks have not ensured that third-party processors and network providers have contingency plans in place to continue operations in the event of a disaster. If an ISO/MSP is providing the backroom operations, examiners should confirm whether management has ensured that the ISO/MSP has a proper contingency plan. The examiner should determine management's practices for requesting and reviewing contingency plans. Further, the merchant processing examination should include IT examiners to the extent needed to review the adequacy of the contingency plan as well as the bank's in-house data processing systems for merchant processing.

Cardholder Information

Cases where disclosure of cardholder information is not in accordance with privacy regulations and the Associations' guidelines warrant scrutiny. Inappropriate disclosure to third parties could result in substantial liability to the bank, especially if the third party perpetrates fraud.

Association regulations prohibit an acquiring bank from disclosing cardholder and transaction information to third parties, other than to its agents for the sole purpose of completing a transaction, without the prior written consent of the cardholder's issuing bank and the Association. The Associations' regulations also state that if an acquiring bank discloses the information, the acquiring bank must ensure that its agents and their employees make no further disclosure and treat the information as confidential.

The emphasis of the privacy regulations is on providing customers a notice of the bank's disclosure practices and an opportunity to opt out of the disclosure. The regulations also prohibit the disclosure of certain cardholder information for marketing purposes, with certain exceptions.

CORRSEPONDENCE WITH THE ASSOCIATIONS

Correspondence between Associations and acquiring banks can point to potential problems with a particular merchant, third-party arrangement, or a significant portion of the acquiring bank's merchant portfolio. Of particular concern are acquiring banks that have been required to post collateral to the Associations, that have had limits placed on their activity, or that have been fined. Associations typically take these actions when the acquiring bank has excessive levels of risk in the merchant portfolio. Topics of correspondence include, but are not limited to:

- Periodic reviews performed on the acquiring bank by an Association.
- High-risk merchants.
- Terminated merchants.
- Excessive volumes of charge-backs at the merchant and bank portfolio levels.

- Fraud or other suspect activity at both portfolio levels.
- Risk limits on activity, or collateral requirements, imposed on the acquiring bank due to the level of risk in the acquiring bank's portfolio.
- Capital requirements.
- Third party usage.

Examiners should closely review correspondence between the bank and the Associations. Banks should also have the applicable Association's by-laws, regulations/rules, and other guidance on hand for review if necessary.

SUMMARY OF EXAMINATION GOALS – MERCHANT PROCESSING

Examiners are expected to determine the level of risk posed by the bank's merchant processing activities as well as determine whether management has correctly identified and is sufficiently controlling those risks with a comprehensive risk management program. In general, the examiner's role includes:

- Reviewing the bank's strategic plan to determine how (and if) merchant processing fits into the bank's objectives.
- Evaluating the bank's merchant processing policies, including, but not necessarily limited to, those covering merchant selection, underwriting, and monitoring.
- Reviewing correspondence between the bank and the Associations regarding the bank's merchant processing activities.
- Determining the quality of the bank's merchant portfolio, including the identification of any high-risk merchants.
- Sampling recently approved (such as within the last 90 days) merchant files.
- Identifying the volume of merchant processing transactions, comparing that volume to the bank's capital level, and determining if additional capital support is necessary.
- Reviewing the trends in the volume and aging of charge-backs, and determining what charge-back losses the bank has suffered.
- Gauging management's ongoing review processes for merchant accounts.
- Evaluating acquiring Rent-a-BIN activities.
- Assessing agent-bank programs and determining level of liability under such programs.
- Analyzing pricing practices and models as well as profitability of the merchant program. Also, considering whether merchant relationships are profitable and investigating as necessary (for example, if a significant relationship is not profitable).
- Reviewing budgeting and forecasting processes for merchant processing activities, including assumptions used.
- Reviewing the settlement flow chart and the bank's practices for paying merchants.
- Identifying what third parties the bank uses for its merchant activities and reviewing controls over third-party risks. The analysis should include reviewing governing contracts or agreements for significant relationships.
- Assessing the adequacy of holdbacks or other merchant reserves.
- Inspecting contingency plans, calling on IT specialists as necessary.
- Reviewing routine MIS for the merchant processing program.
- Assessing whether management possess the necessary skill-sets to properly management the program.
- Reviewing fraud detection procedures.
- Reviewing merchant program sections of internal and external audit reports.
- Determining whether any planned changes exist for the merchant operation. If changes are planned, identify how the changes may impact the bank, specifically as related to higher risks that the bank may be taking on.